数学基礎論の世界

ロジックの雑記帳から

竹内外史

日本評論社

まえがき

本書の内容は『数学セミナー』誌に，‘私の雑記帳から’という題名で連載されたもの（‘初等初等整数論’(1971年5，6，7月号)，‘有限の立場について’(同年10月号)，‘ウント大きな自然数’(同年11月号)，‘ニセモノ自然数’(同年12月号))，トピックスとして連載された‘ゲーデルの新しい公理について’(1971年8，9月号)，『栃木県数学教育同好会資料 No. 26』(1970年）のために書かれた‘自然数論におけるある決定問題’に新たに‘体の理論とロジック’を付け加えてできたものである．

‘私の雑記帳から’の連載のはじめにつぎのように書いたがこれが本書全体に流れる雰囲気であるといってよいであろう．

> 雑記帳をひろげてみるというのは，なかなか面白いものである．こんなことが書いてあったかと思うような意外なことが書いてあったりする．正統的な教科書には書いてないようなことで一面からいえばムダな時間つぶしにしかならないが，反面，逆により教育的ともいえないこともない．これから6回にわたって‘私の雑記帳から’という題でいろいろなことについて話をしてみたい．落書でも見る気持で読んでいただければ幸いである．

この機会にもう少し付け加えさせていただくとつぎのようになる．いつも正統的な教科書を用いて講義をしているとつぎのような不満がでてくる．教

科書にでていることは成程一番基本的な大切なことにちがいないが，何かその分野の雰囲気を伝えるためには物足りなく感じられることも多い．たとえ本筋からハズレても，こういうことも伝えたくもあるということがたくさんある．こういうことを初心者には入門書となるように，また，いま正統的な教科書を読んでいる人または正統的な教科書を一通りすました人には課外の副読本となるようなものを書いてみたらどうだろうか？　この希望がどの程度到達できたか私にはわからないが，本書によって幅広いロジックへの理解，またはふつうの教科書からは得られない刺戟を得られる人があるとすれば筆者にとっては望外の喜びである．

本書をつくる企画中に出版社から大幅に新しいことを付け加えてよいというので，‘体の理論とロジック’を付け加えた．私達は常に数学というのは有機的につながった一つの学問であっていろいろ異なった分野が互いに関連しあい，刺戟しあって成長してゆくものと信じているのであるが，いまだにこういうふうに数学有機体を考えるときにロジックは数学の外にハズシテ考える人が少なくない．数学という名がついても高々‘ニセモノ数学’(これは‘ニセモノ自然数’という題名を見てある大先生がいかにもうれしそうにおっしゃられた言葉である）くらいにしか思っていない人が多い．整数論および代数学はわが国で盛んな分野であるから，こういうササヤカな努力が上のような偏見を打破する一助となればと思ってのことである．

あとがきに‘ゲーデルの新しい公理について’の現在までに私が知っている主な発展について書いておいた．こういう現代数学史の裏側にかくれてゆくトピックスを成書にとりあげることの疑問は当然あることであるが，私としてはやはり消え去ってゆく前に書き残しておきたくもある．また中途半端な現在までの情報を伝えることがよいかどうかもわからないが，やはり機会があたえられるごとに報告してゆくのも義務であるような気がする．

最後に本書についての著者の個人的な感情を書いておきたい．‘ゲーデルの新しい公理について’，‘有限の立場から’，‘初等初等整数論’はこの順に1971年１月に１学期の授業がすんで２月からの２学期の授業の始まる前に書

いたものである，‘ウント大きな自然数’，‘ニセモノ自然数’は同年5月にもう1年の授業が全部すんでホットした気分で書いたものである．‘自然数論における ある決定問題’はもちろん1970年の夏休みに，また，‘体の理論とロジック”は付け加えてよいということになって大急ぎに1971年の感謝祭の休日に書いたものである．いずれにしても私には休日の思い出につながるものである．無用な誤解を避ける為に付け加えておくが，本書に書いたようなことを書いた雑記帳を私がもっている訳ではない．私の雑記帳には，やりかけの計画，失敗した計算の名残りなどが雑然と書いてあるだけである．

‘私の雑記帳から’の『数学セミナー』誌への連載は矢野健太郎教授のお勧めにしたがったものであり，『数学セミナー』連載中は日本評論社野田幸子，西原昌幸の両氏に大変お世話になった．また‘自然数論におけるある決定問題’の栃木県数学教育同好会に資料として発表の時には同会の榎本和平氏夫妻にいろいろと御手数を煩わした．さらに本書の出版の際には日本評論社東弘幸，金沢公子の両氏に大変お世話になった．これらの方々にここに厚く感謝の意を表したい．

1972年3月　プリンストンにて

竹 内 外 史

目次

初等初等整数論

トコトンまでわかる自然数論

初等初等整数論というのは，初等整数論のミスプリントではない．いままですでに初等整数論というだいたいに確定した分野があって，それよりはずっと易しいことなので初等初等整数論といったのである．

ここでやろうとすることは，最後の最後までハッキリわかったと思える数学をやろうということである．だいたい数学はむずかしすぎる．すべての実数の集合なんていったって全部並べて調べるわけにはいかないし，何のことをいっているのかサッパリわからない．もっと簡単に実数などといったって，ボンヤリとした直線のイメージがあるところへ頭ごなしにむずかしい公理をおしつけてこられる．やりきれたものではない．

いつもおしつけがましい消化不良の数学ばかりやらないで，タマにはトコトンまでよくわかる数学をやってみたらどうだろうか？

どうも数学にはむずかしい概念が多すぎる．数学はイザとなれば一歩一歩論理的にきちんと証明できるから，時間さえかければ誰にでも一通りはわかるようになるというけれども，たいていの場合は急にむずかしい概念が天から降ってきて，それがどういうことかよく理解しなければ結局は外国語をきいているようなもので，何をいっているのかわからない．

ところで数学者は意地悪にできているから，その概念を用いてできた長い

定理か理論がすんだあとでなければ，その概念の意味がわからないようになっている．数学者というのは，どうもサディストかマゾヒストがそろっているらしい．

だいたい，入り易いといわれている，群論や位相空間論にしてもそうだ．一番はじめにいうことが，しかじか，かくかくの条件をみたしているものを群という．そんなことをいったって，どんな化け物のような群があるかわかったものではない．結局は何を考えているのかわからないものについて考えさせられて，そのうえにむずかしい定義がドカドカと降ってくるのである．

こんなことは，もうすっかりやめてしまいたい．文明の世からは遠ざかっても，見るもの聞くものよく知ったものばかりの素朴な生活がしてみたい，というわけで初等初等整数論をやろうというのである．

まず戦争廃止というように，禁止協定を作ろう．まずむずかしいものはやめよう，賛成，もっとハッキリいって，集合などというむずかしいものはやめてしまおう．むずかしい概念や定義もやめてしまおう．禁止協定の条文がアイマイだと，また頭のよい数学者が変な抜道を考えるといけないから，もっとハッキリと禁止することにしよう．

だいたい，数学の概念はその理論の基本的な概念から論理記号を組み合わせてできている．論理記号は

$\neg$（でない），　$\wedge$（そして），　$\vee$（または），

$\rightarrow$（ならば），　$\forall$（すべて），　$\exists$（存在する）

だ．このうちで $\neg$，$\wedge$，$\vee$ はよい．もとの命題が正しいか，間違っているか？ がわかればいつでも，正しいか間違っているかが計算できるし，意味がハッキリわかっている．$A\rightarrow B$ は $\neg A\vee B$ だと思えばよいから，まあよいということにしよう．問題なのは $\forall$ と $\exists$ だ．いつでもこれがでて話がむずかしくなってきてしまう．面倒だから $\forall$ と $\exists$ は一切用いないことにしよう．

さて，しようというだけではものたりないから，憲法のようにキチンと条文にすることにしよう．

1.　基本的な概念から新しい概念を作るとき， $\neg, \wedge, \vee, \rightarrow$ を用いてもよいが， $\forall$ と $\exists$ は絶対に用いてはいけない．

こういうふうにすると，大分ハッキリしてきたような気がする．しかしちょっと心配にもなってくる．条文だけができて何もすることがないでは困るのだが，$\forall$ も $\exists$ もないとすると，いったい数学のなかで何かすることがあるだろうか？　あるある．

$$(a+b)^2=a^2+2ab+b^2$$

というのがある．これからは，こういうのばかりやることにしよう．さて，うっかりすると，変なことになるかもしれない．変数の意味は何だろう．その変数にどんな数を入れても正しいという普通の意味でよいだろう．

もう何をやっているかわからないものについて考えるのはコリゴリだ．考えるものをはっきり決めてしまおう．数学は数についての学問だから，数について考えるのがよいだろう．だけども実数はむずかしすぎる．第一もうすでに何のことかわからない．有理数も面倒だ．整数もマイナスというのが気に入らない．いっそのこと自然数だけということにしてしまおう．まてよ，自然数といってもまた公理などというのをおしつけられてはやりきれない．といって 10 進法というのもキチンとのべると大変だ．ここでは自然数とは

$$0,\ 0',\ 0'',\ 0''',\ \cdots$$

ということに決めてしまおう．もっとも $0'''$ などと書くのは面倒だから，これは原理上ということにして，実際には

$$0,\ 1,\ 2,\ 3,\ \cdots$$

を使うことにしよう．

さて，こういうふうにガンバッても自然数についての基本的な関係についてやっかいなものを許したのではナンニモならない．だいたいいままで $\in$ というのにサンザンいじめられてきた．ここでは一番カンタンで誰でも知っているもの

$$=$$

だけということにしよう．これならほんとうに安全だ．２つの自然数 n と m とをとってきたとき，いつでも $n=m$ が正しいかどうかは判定できるもの．

さて，これで全部すんだかな．何か抜けているような気がする．そうだ $+$ と $\cdot$ が抜けている．関数というのが抜けている．$+$ と $\cdot$ は入れることにしよう．まてまて頭ごなしに入れてはいけない．徹底的にチェックして，トコトンまでわかるということがわかってからでないと入れてはならない．ということはどういうことかな．どうやらキチンと定義ができて，定義の意味がよくわかるということらしい．いったい $+$ の定義はどうするのだろう．残念なことに小学校では習わなかった．これはキチンと考えよう．$a+b$ の定義は何だろう．まず b が 0 のとき，$a+0$ はこれは a だ．b が 0 でないときは，b は n' という形をしているわけだが．

$a+n'$ はこれは $a+n$ の次の数 $(a+n)'$ だ．

これで全部の場合がつきたから

$$a+0=a,$$

$$a+n'=(a+n)'$$

で，$+$の定義ができているはずだが，ほんとうにこれでよいかしら．いま勝手に a と b とをとってくると，b が 0 ならば $a+b$ は a と計算ができる．b が n' とすると $a+b$ は $(a+n)'$ だから，$a+n$ の計算ができればよい．

ところでこれは１つ手前のカンタンな自然数の計算にもどったのだから，こうして順々に１つ手前，１つ手前ともどしていけば，しまいには $a+0$ の計算にもどってしまう．だから，上の規則は計算の規則をのべたもので，a と b とがあたえられたら，いつでも $a+b$ が 1 通りに計算できるから，どうやらハッキリわかっているといってよさそうだ．だけども，どうも上の規則は見た目が悪い．どうしてだろう．どうも a の次の自然数を a' と書くのが悪いらしい．せっかく，$+$ ができたのだから，これから a' と書かずに $a+1$ と書くことにしよう．そうして上の規則を書き直すことにしよう．

2.
$$a+0=a,$$
$$a+(n+1)=(a+n)+1$$

さて，それでは・はどうだろう．＋と同じことをやってみたらどうだろう．

3.
$$a\cdot 0=0$$
$$a\cdot(n+1)=a\cdot n+a$$

いま勝手な自然数 a と b とをとってきたとき，これで $a\cdot b$ が計算できるかどうか？　まず b が 0 ならば，これはよい．b が 0 でなければ，n' そうだ $n+1$ だから，$a\cdot(n+1)=a\cdot n+a$ で $a\cdot n$ と ＋ の計算にもどってしまう．＋ の計算の仕方はもうわかっているから，これは $a\cdot n$ が計算できればよい．これは1つ手前の n についての乗法の計算にもどったのだから，こうして順々にもどしていけば，しまいには $a\cdot 0$ の計算になって，できてしまう．しかし，こうやってみると，ほかにも同じことができそうである．ひとつ巾（ベキ）についてやってみよう．

4.
$$a^0=1$$
$$a^{n+1}=a^n\cdot a$$

理屈はまったく同じことである．いつもハッキリ計算ができるし，計算の仕方も明瞭である．

一般の場合を考えてみよう．g と h という関数がもうすでにあたえられて，計算の仕方がハッキリわかっており，いつでも計算できるものとする．このときに f という関数をつぎの計算の仕方をあたえることで定義するのである．

5.
$$f(a_1,\cdots,a_t,0)=g(a_1,\cdots,a_t)$$
$$f(a_1,\cdots,a_t,n+1)=h(a_1,\cdots,a_t,n,f(a_1,\cdots,a_t,n))$$

この f という関数の計算の仕方を考えてみる．いま勝手な自然数 $a_1, \cdots, a_l, b$ があたえられたとして，

$$f(a_1, \cdots, a_l, b)$$

の計算をすることを考えてみよう．b が 0 ならば，これは $g(a_1, \cdots, a_l)$ で g の計算の仕方はわかっているからよい．b が 0 でなければ，これは $n+1$ の形であろう．ところで，これは

$$h(a_1, \cdots, a_l, n, f(a_1, \cdots, a_l, n))$$

となり，h の計算の仕方はすでにわかっているから，$f(a_1, \cdots, a_l, n)$ の計算をすることに問題は還元されたことになる．n は b の 1 つ手前の自然数であるから，これを順々にくり返せば，しまいには $f(a_1, \cdots, a_l, 0)$ の計算に還元されて計算が完了する．

このように上の方法で導入された関数は必ず計算して値を求めることができるし，この計算の仕方もハッキリわかっているので，これはハッキリわかっているといってよいであろう．ほかにもハッキリわかる関数があるかもしれないが，あまり手をひろげるのは物騒だから考える関数は a' という関数からはじまってこの方法で導入されるものだけにかぎることにする．

さて，こう何もかにも制限するとちょっと心配になってくる．われわれのやることは関数の計算をすることだけで，それ以外に数学らしいものはないのではないか？ ということである． これならば簡単な関数の計算のプログラムを作って，それで終りということになってしまう．いくらむずかしいことがきらいでも，これではちょっと味気ない．少しばかり心配だから，よく知っていることをとりだして少し調べてみる．加法の交換律

6.	$a+b=b+a$

というのがある．これは少なくとも上の $+$ の計算の規則からは自明ではない．大ゲサにいえば定理といってよさそうだ．いったいどうやって証明するのだろうか？

いままでと同じようにやって，まず $b=0$ のときは

7.　$a+0=0+a$

これは，$a+0$ は a だから

$$a=0+a$$

をいえばよいのだが，これはどういったらよいだろうか？

普通の証明は？　普通の証明は数学的帰納法でやるのである．すなわち

$$a \text{ が } 0$$

のときは

$$0+0=0$$

だからよろしい．

$$a \text{ が } n+1$$

の形のときは

$$0+(n+1)=(0+n)+1=n+1$$

となってよろしい．

ところで数学的帰納法というのは，ほんとうによいのだろうか？

こんなところで**数学的帰納法**の公理というのを天下りに入れたのではいままでの苦労が水の泡になってしまう．

いまこの証明を $b=3$ のときにチェックしてみよう．全部くり返すと長くなるから，肝心の筋道だけを抜きだすと，

$$0+0=0 \quad \text{だから} \quad 0+1=1$$

$$0+1=1 \quad \text{だから} \quad 0+2=2$$

$$0+2=2 \quad \text{だから} \quad 0+3=3$$

$$\text{ゆえに} \quad 0+3=3$$

という議論をしていることになる．してみると，われわれの場合は数学的帰納法といっても，何も公理といってさわぐことはない．b についての数学的帰納法というのは，b が 0 のときはあたりまえ，b が 0 のときは正しいから，しかじかかくかくの理由で b が 1 のときも正しい，b が 1 のとき正しいから，同じくしかじかかくかくの理由で b が 2 のときも正しい … とただ同じ議論をバカのように何度もくり返すだけにすぎず，だから数学的帰納法はそのつどその意味がトコトンまでわかるわれわれの数学にふさわしい

ものといってよいであろう．

数学的帰納法が入ってくると，一挙にたくさんの定理が証明できるようになる．少しばかりやってみよう．

8.	$(a+b)+c=a+(b+c)$

c についての数学的帰納法で証明する．

$$c \text{ が } 0$$

のときは

$$\text{両辺とも } a+b$$

になるから明らかである．

$$c \text{ が } n+1$$

のときは，帰納法の仮定 $(a+b)+n=a+(b+n)$

を用いて

$$\begin{aligned}(a+b)+(n+1)&=((a+b)+n)+1 && \text{(2. を用いた)}\\ &=(a+(b+n))+1 \\ &=a+((b+n)+1) && \text{(2. を用いた)}\\ &=a+(b+(n+1)) && \text{(2. を用いた)}\end{aligned}$$

となって証明完了である．

9.	$a+1=1+a$

a についての数学的帰納法で証明する．

$$a \text{ が } 0$$

のときは

$$\text{両辺とも } 1$$

で明らかである．

$$a=n+1$$

のときは帰納法の仮定 $n+1=1+n$

を用いて

$$(n+1)+1=(1+n)+1=1+(n+1)$$

最後の等式は 8. を用いたのである．

さて，いよいよやりかけの $a+b=b+a$ をやることにする．これを b に

ついての数学的帰納法で証明することにする．まず

$$b \text{ が } 0$$

のときは

$$a+0=0+a$$

ですでに証明されているからよい．つぎに

$$b \text{ が } n+1$$

のときは帰納法の仮定 $a+n=n+a$ を用いて

$$\begin{aligned} a+(n+1) &= (a+n)+1 \\ &= (n+a)+1 \\ &= n+(a+1) && \text{(8. を用いた)} \\ &= n+(1+a) && \text{(9. を用いた)} \\ &= (n+1)+a && \text{(8. を用いた)} \end{aligned}$$

となって証明が完了する．

さて数学的帰納法といっても，数学のなかには，なかなかコッタ数学的帰納法もある．数学的帰納法の名のもとにむずかしいものをもちこまれても困る．ここでふたたび条文化して危険を防止することにしよう．いったいどうのべたらよいであろうか？ 普通の表現では

$$\frac{A(0) \qquad A(a)\to A(a+1)}{\forall x A(x)}$$

すなわち $A(0)$ がいえて，また任意の a について $A(a) \to A(a+1)$ がいえるならば $\forall x A(x)$ がいえる，というのであるが，これはわれわれの場合はいけない．すなわち結論に $\forall$ が入ってきてわれわれの平和憲法第一条に反するのである．素朴なわれわれの平和を保つためにわれわれは $\forall x A(x)$ と書くかわりに，どんな自然数 n をとってきても $A(n)$ がいえるという形に書くことが必要である．もっとも，これは n のような形でなくても，b という変数の形でもよいであろうし，$b+c$ というような形でもよいであろう．

もう 1 つ重大な注意は，はっきりのべなかったがこの $A(a)$ のなかには $\forall$ や $\exists$ は入っていない．入っているのは変数と，0 と，われわれが許可した関数と $=$ に $\neg$，$\vee$，$\wedge$，$\to$ だけであるということが大切である．この注意はきわめて大切である．さらに変数と 0 とわれわれが許可した関数とだ

けから組み合わされてできたものを term といって，これを t で表わすこととしよう．term はもし変数に自然数を代入すれば，いつでもどのように計算をするかがわかっていて答を求めることができる．このうえでつぎのように数学的帰納法を条文化することができる．

10.　数学的帰納法

$$\frac{A(0) \qquad A(a) \to A(a+1)}{A(t)}$$

ここに $A(a)$ はわれわれの許可した命題：すなわち 0 と変数とわれわれの許可した関数と ＝ と ¬，∨，∧，→ だけを組み合わせた命題であり，t はわれわれの意味での任意の term である．さらに $A(0)$ には a という変数は入っていないとする．（これは $A(a) \to A(a+1)$ が任意の自然数 a に対して正しいという意味から当然である．）

さて数学的帰納法のほかにもわれわれの数学にふさわしい方法があるかもしれない．しかしちょっと考えたところでは気がつかない．アイマイにしておくと，どんな危険なものが混入してくるかもしれない．一応これで全部ということにして，このわれわれの気に入った数学のなかで，どれだけのことができるか？　少しばかりやってみたいと思う．

初等初等整数論の遂行

いままでお膳立てをしたなかで，実際に数学をやってみることにする．実際の目的は普通初等整数論といわれるものをできるだけたくさんやってみせるということであるが，文明から遠ざかった罰として，いろいろと不自由なこともたくさんある．また，その不自由を補うためにいろいろなことをしなければならない．ちょうどロビンソン・クルーソーが孤島にいって簡単な道具を全部自分で作り直さなければならないようなものである．

いままでに証明したものはもちろんどんどん用いるし，だいたい同じような方法で証明できるものは遠慮なしに省略することにするから，慣れない人

は演習問題だと思って自分で証明をつけていただきたい．

また多少とも数学の心得のある人には，非文明の生活は万事がノロク，不便であろうが，しばらく辛抱をしていただきたい．こういうことをやることの意味，それについての全体的な考察は，そのあとでくることであるから．いままでの定義，定理は全部そのままにして，ここからはじまる定義，定理だけをあらためて番号をつけていくが，これ以前のものを邪魔にしているわけではない．

まずだいたいにおいて，数学的帰納法を順々に用いれば容易にできることとして（定理の順序が大切である．すなわち後の定理の証明には前の定理がよく用いられる）

定理 1
$$a\cdot(b+c)=a\cdot b+a\cdot c$$

定理 2
$$a\cdot(b\cdot c)=(a\cdot b)\cdot c$$

定理 1 と定理 2 は c についての数学的帰納法を用いる．

定理 3
$$0\cdot a=0$$

定理 4
$$1\cdot a=a$$

定理 3 と定理 4 は a についての数学的帰納法を用いる．

定理 5
$$(a+b)\cdot c=a\cdot c+b\cdot c$$

定理 5 は c についての数学的帰納法で証明する．

定理 6
$$a\cdot b=b\cdot a$$

定理 6 は b についての数学的帰納法で証明する．ちょっとした注意をしておくと定理 2 を定理 1 を抜かして直接証明しようとするとなかなかできないし，定理 6 を定理 5 を抜かしてやろうとするとやはりなかなかできない．

定理 7
$$a^{(b+c)}=a^b\cdot a^c$$

定理 8
$$(a^b)^c=a^{bc}$$

定義 1
$$\mathrm{pd}(0)=0$$
$$\mathrm{pd}(a+1)=a$$

この定義が 5 の関数の定義の特別な場合であることをしかと確かめていただきたい．もちろんこの関数の計算は容易であろう．もちろん $\mathrm{pd}(a)$ はだい

たいにおいて $a-1$ であるがこれは a が 0 のとき -1 とはおけない（われわれはいま負の数を考えていない）ので，そのときは 0 とおくのである．pd は predecessor（前者）の略である．

定義 2

$$a \dot{-} 0 = a$$

$$a \dot{-} (n+1) = \mathrm{pd}(a \dot{-} n)$$

$a \dot{-} b$ は $a-b$ にほとんど同じであるが，b が a より大きいときはその値を 0 とおくのである．

定理 9

$$a=0 \vee \mathrm{pd}(a)+1=a$$

（証明）　a を 0 の場合と $n+1$ の形のときに分ければよい．

定理 10

$$(a \dot{-} b) \dot{-} c = a \dot{-} (b+c)$$

（証明）　c についての数学的帰納法．

定理 11

$$a \dot{-} b = 0 \vee (a \dot{-} b)+b=a$$

（証明）　b についての数学的帰納法を用いる．

$$b=0$$

とすれば，

$$(a \dot{-} 0)+0=a$$

であるから明らかである．

$$b=n+1$$

とすれば，帰納法の仮定より

$$a \dot{-} n=0 \vee (a \dot{-} n)+n=a$$

いま

$$a \dot{-} n=0$$

とすれば

$$a \dot{-} (n+1) = \mathrm{pd}(a \dot{-} n) = \mathrm{pd}(0) = 0$$

となって定理は成立するから

$$a \dot{-} n \neq 0 \wedge (a \dot{-} n)+n=a$$

とする．定理 9 より

$$\mathrm{pd}(a \dot{-} n)+1 = a \dot{-} n$$

ところで

$$\begin{aligned}(a \dot{-} (n+1))+(n+1) &= \mathrm{pd}(a \dot{-} n)+1+n \\ &= (a \dot{-} n)+n\end{aligned}$$

$$=a$$

定理 12
$$a+c=b+c \rightarrow a=b$$

（証明）　c についての数学的帰納法.

定理 13
$$a+b=0 \rightarrow a=0 \wedge b=0$$

（証明）　b についての数学的帰納法.

定理 14
$$a\dot{-}(a+b)=0$$

（証明）
$$\begin{aligned} a\dot{-}(a+b)\neq 0 &\rightarrow (a\dot{-}(a+b))+(a+b)=a \\ &\rightarrow (a\dot{-}(a+b))+b=0 \\ &\rightarrow a\dot{-}(a+b)=0 \end{aligned}$$

定理 15
$$a\dot{-}b=0 \vee b\dot{-}a=0$$

（証明）
$$\begin{aligned} a\dot{-}b\neq 0 &\rightarrow (a\dot{-}b)+b=a \\ &\rightarrow b\dot{-}a=b\dot{-}(b+(a\dot{-}b))=0 \end{aligned}$$

定理 16
$$(a+1)\dot{-}(b+1)=a\dot{-}b$$

（証明）　b についての数学的帰納法.

定理 17
$$b\dot{-}a=0 \rightarrow (b+c)\dot{-}(a+c)=0$$

（証明）　c についての数学的帰納法.

定理 18
$$(b+c)\dot{-}a=0 \rightarrow b\dot{-}a=0$$

（証明）
$$\begin{aligned} b\dot{-}a\neq 0 &\rightarrow (b\dot{-}a)+a=b \\ &\rightarrow 0=(b+c)\dot{-}a=((b\dot{-}a)+c+a)\dot{-}a \\ &\qquad =(b\dot{-}a)+c \\ &\rightarrow b\dot{-}a=0 \end{aligned}$$

定義 3　　$a\leqslant b$ を $a\dot{-}b=0$

のことと定義する.

ここに注意すべきことは，われわれは $\exists$ を用いることができないから，$a\leqslant b$ を $\exists x(a+x=b)$ と定義するわけにはいかないのである.

$$a<b$$

を
$$a\leqslant b \wedge a\neq b$$

と定義する.

定理 19

1)　$$a \leqslant a+b$$

2)　$$a \leqslant b \vee b \leqslant a$$

3)　$$b+c \leqslant a \to b \leqslant a$$

（証明）　いずれも定理 14, 15, 18 の書きかえである．

定理 20　$$b \dot{-} a=0 \to a=b+(a \dot{-} b)$$

（証明）　a についての帰納法による．

$$a=0$$

のときは，$$b \dot{-} 0=0$$

から　$$b=0$$

がでて定理は明らかである．

$$a=n+1$$

とするとき，$b=0$ ならば明らかであるから，$b \neq 0$ とすると，

$$b=\mathrm{pd}(b)+1.$$

$$0=b \dot{-}(n+1)=(\mathrm{pd}(b)+1) \dot{-}(n+1)=\mathrm{pd}(b) \dot{-} n$$

$$\to n+1=(\mathrm{pd}(b)+(n \dot{-} \mathrm{pd}(b)))+1$$

$$=(\mathrm{pd}(b)+1)+((n+1) \dot{-}(\mathrm{pd}(b)+1))$$

$$=b+((n+1) \dot{-} b)$$

定理 21　$$\mathrm{pd}(a)=0 \to a=0 \vee a=1$$

（証明）　a についての数学的帰納法により明らか．

定理 22　$$a \dot{-} b=0 \wedge b \dot{-} a=0 \to a=b$$

（証明）　b についての数学的帰納法で行なう．

$$b=0$$

のときは明らかであろう．

$$b=n+1$$

とすると　$$a \dot{-}(n+1)=0 \to a \dot{-} n=0 \vee a \dot{-} n=1$$

いま　$$a \dot{-} n=1$$

とすると　$$a=n+(a \dot{-} n)=n+1$$

となって，証明ができるから $a \dot{-} n=0$ から矛盾をだせばよい．ところで一方

$$(n+1) \dot{-} a=0 \rightarrow n \dot{-} a=0 \qquad \text{(定理 18)}$$

ゆえに帰納法の仮定より　$a=n$

となり　$(n+1) \dot{-} a=1$

となって　矛盾する．

定理 23　$a \leqslant b \wedge b \leqslant a \rightarrow a=b$

(証明)　これは前定理の書き直しである．

定理 24　$a \dot{-} b=0 \wedge b \dot{-} c=0 \rightarrow a \dot{-} c=0$

(証明)　$a \dot{-} c \neq 0$

とすれば　$c+(a \dot{-} c)=a$

ゆえに　$a \dot{-} b=0$

から　$c \dot{-} b=0$

がでる．

　これと　$b \dot{-} c=0$

とあわせて　$b=c$

ゆえに　$a \dot{-} b \neq 0$

が $a \dot{-} c \neq 0$ からでて　矛盾する．

定理 25　$a \leqslant b, b \leqslant c \rightarrow a \leqslant c$

(証明)　これは前定理の書き直しである．

　これでやっと $\leqslant$ のだいたいの性質がでて楽になった．

定理 26　$a \leqslant b \rightarrow a+c \leqslant b+c$

(証明)　定理 17 より明らか．

定理 27　$a \leqslant b \wedge c \leqslant d \rightarrow a+c \leqslant b+d$

(証明)　定理 25 と定理 26 より明らか．

定理 28　$a \leqslant b \rightarrow a \cdot c \leqslant b \cdot c$

(証明)　c についての数学的帰納法による．

このつぎにはこの初等初等整数論をもう少し展開して，それからわれわれはいったいどんなことをしているのかを少し考えてみることにしよう．

初等整数論の入口まで

前節で大小の概念が入ったのでだいぶ楽になった．ロビンソン・クルーソーの非文明の生活も多少の道具ができて，キチンキチンとした生活ができるようになったというところである．これで大小についてのことはたいていは普通のようにできるようになった．試みにつぎの演習問題をやってみていただきたい．

演習問題　$a<b \wedge 0<c \rightarrow a\cdot c<b\cdot c$

しかしながら，いくらなんでも大小だけでは情ない．やはり整数論とかりにも名前をつけた以上は，多少は整数論らしい感じのするところまではやってみたい．もう一押しガンバッてみることにしよう．

定義 4　$\min(a, b)=b \dot{-} (b \dot{-} a)$

$\min(a, b)$ は‘a と b とのなかで小さい方’という意味である．この定義がこの意味を表わしていることはつぎの定理で明らかであろう．

定理 29

1)　$a \leqq b \rightarrow \min(a, b)=a$

2)　$b \leqq a \rightarrow \min(a, b)=b$

（証明）1）は

$$a \leqq b$$

を仮定すれば前節の定理 20 より

$$b=a+(b \dot{-} a)$$

したがって　$b \dot{-} (b \dot{-} a)=(a+(b \dot{-} a)) \dot{-} (b \dot{-} a)$　（定理 17 を用いる）

$$=a$$

となって証明された．また

2）のほうは

$$b \leqq a$$

から

$$b \dot{-} a=0$$

がでるから明らかである．

この定理からつぎの定理は明らかであろう．

定理 30　$\min(a,b)=\min(b,a)$

同様の流儀で‘a と b とのなかで大きい方’を $\max(a,b)$ と表わすことにしてつぎのように定義する．

定義 5　$\max(a,b)=(a+b)\dot{-}\min(a,b)$

前節の定理 17 と上の定理 29 よりつぎの定理は明らかであろう．

定理 31

1)　$a\leqq b \to \max(a,b)=b$

2)　$b\leqq a \to \max(a,b)=a$

3)　$\max(a,b)=\max(b,a)$

定義 6

1)　$\min(a_1,\cdots,a_n)=\min(\cdots\min(\min(a_1,a_2),a_3)\cdots,a_n)$

2)　$\max(a_1,\cdots,a_n)=\max(\cdots\max(\max(a_1,a_2),a_3)\cdots,a_n)$

$\min(a_1,\cdots,a_n)$ は‘$a_1,\cdots,a_n$ のなかで一番小さいもの’を表わし，$\max(a_1,\cdots,a_n)$ は‘$a_1,\cdots,a_n$ のなかで一番大きいもの’を表わすことは明らかであろう．$\min(a_1,\cdots,a_n)$ や $\max(a_1,\cdots,a_n)$ が $a_1,\cdots,a_n$ の並べ方の順序に関係しないなどの性質があるが，いずれも証明はほとんど明らかなので省略することにする．

定義 7　$\mathrm{sg}(0)=0$

$\mathrm{sg}(a+1)=1$

この新しい関数 sg の定義が前節にのべた関数の定義の特別な場合であることを確かめてほしい．sg は 0 のときは 0，それ以外は 1 という関数であって sg は signature（符号）の略である．すなわち 0 か正かを伝える関数である．

定義 8　$\overline{\mathrm{sg}}(a)=1\dot{-}\mathrm{sg}(a)$

$\overline{\mathrm{sg}}(a)$ は a が 0 ならば 1，それ以外は 0 という関数であることはただ

ちにわかるであろう．

定義 9　$$|a-b|=(a\dot{-}b)+(b\dot{-}a)$$

慣用のように，$|a-b|$ は '$a-b$ の絶対値' を表わす．

ただちにつぎのことがわかる．

$$a\leqslant b \rightarrow |a-b|=b\dot{-}a$$

$$b\leqslant a \rightarrow |a-b|=a\dot{-}b$$

さて，いままで，加法，乗法，減法，大小とやってきた．そろそろ割り算もやってみたいものである．ところで割り算はわれわれの体系ではそれほど簡単ではない．まず a を b で割ったときの余りだけを表わすことを最初に考えよう．剰余は英語で remaincer であるので，これを $\mathrm{rm}(a,b)$ で表わすことにしよう．

定義 10　$$\mathrm{rm}(0,b)=0$$

$$\mathrm{rm}\,(a+1,b)=(\mathrm{rm}\,(a,b)+1)\cdot\mathrm{sg}|b-(\mathrm{rm}\,(a,b)+1)|$$

まず，この定義がわれわれの関数の定義に従っていることを注意されたい．$\mathrm{rm}\,(a,b)$ の定義は a が 0 のときは問題はないとして，$\mathrm{rm}\,(a+1,b)$ は $\mathrm{rm}\,(a,b)+1$ が b より小さければ $\mathrm{rm}\,(a,b)+1$ のことであり，$\mathrm{rm}\,(a,b)+1$ が b となれば 0 であるということは知りつくしていることであるから，上の定義がわれわれの知っている剰余と同じものであることはただちにわかるであろう．しかしながら，剰余についてのいろいろな性質は，もちろんキチンと証明しなければならない．

定理 32　$$0<b \rightarrow \mathrm{rm}\,(a,b)<b$$

（証明）　a についての帰納法で証明する．

$$0<b$$

を仮定する．

$$a=0$$

のときは，$$\mathrm{rm}\,(a,b)=0$$

であるから明らかである．

つぎに，$\mathrm{rm}\,(a,b)<b$

を仮定して，$\mathrm{rm}\,(a+1,b)<b$ を証明しよう．

$$\mathrm{rm}\,(a,b)<b$$

から $\mathrm{rm}\,(a,b)+1\leqq b$

$$\mathrm{rm}\,(a+1,b)\leqq \mathrm{rm}\,(a,b)+1$$

は定義から明らかであるから，$\mathrm{rm}\,(a,b)+1<b$ であれば証明は完了したと思ってよい．したがって

$$\mathrm{rm}\,(a,b)+1=b$$

の場合だけ考えればよい．このときは，

$$\begin{aligned}\mathrm{rm}\,(a+1,b)&=(\mathrm{rm}\,(a,b)+1)\cdot\mathrm{sg}\,|b-(\mathrm{rm}\,(a,b)+1)|\\&=0 \qquad (|b-(\mathrm{rm}\,(a,b)+1)|=0\ \text{だから})\end{aligned}$$

となって $\mathrm{rm}\,(a+1,b)<b$

が証明された．

定理 33 $\mathrm{rm}\,(a,0)=a$

（証明）a についての帰納法で簡単に証明される．

つぎに割り算の商を考えることにする．a を b で割ったときの商を $[a/b]$ と書くことにすると，

定義 11 $[0/b]=0$

$$[(a+1)/b]=[a/b]+\overline{\mathrm{sg}}\,|b-(\mathrm{rm}\,(a,b)+1)|$$

これもわれわれの関数の定義の特別な場合になっている．

$[0/b]=0$ の意味は明らかであろう．第 2 式の意味は $[(a+1)/b]$ が $[a/b]$ より 1 だけ増えるのは，$\mathrm{rm}\,(a,b)+1$ が，ちょうど b になるときである，ということであり，われわれのよく知っている知識に適応する．

定理 34 $a=[a/b]\cdot b+\mathrm{rm}\,(a,b)$

（証明）a についての帰納法で証明する．

$$a=0$$

のときは明らかだから，

$$a=[a/b]\cdot b+\mathrm{rm}\,(a,b)$$

を仮定して　$a+1=[(a+1)/b]\cdot b+\mathrm{rm}\,(a+1,b)$　を証明することにする．場合を 2 つに分けて考える．

$\mathrm{sg}|b-(\mathrm{rm}\,(a,b)+1)|=0$　のとき

このときは　$\overline{\mathrm{sg}}|b-(\mathrm{rm}\,(a,b)+1)|=1$　と　$b=\mathrm{rm}\,(a,b)+1$

がわかるから定義より

$$[(a+1)/b]=[a/b]+1 \quad と \quad \mathrm{rm}\,(a+1,b)=0$$

とがでてくる．ゆえに

$$\begin{aligned}[(a+1)/b]\cdot b+\mathrm{rm}\,(a+1,b)&=[a/b]\cdot b+b\\&=[a/b]\cdot b+\mathrm{rm}\,(a,b)+1\\&=a+1\end{aligned}$$

となって証明された．

$\mathrm{sg}|b-(\mathrm{rm}\,(a,b)+1)|=1$　のとき

このときは　$\overline{\mathrm{sg}}|b-(\mathrm{rm}\,(a,b)+1)|=0$

となるから定義から　$[(a+1)/b]=[a/b]$

$$\mathrm{rm}\,(a+1,b)=\mathrm{rm}\,(a,b)+1$$

がわかる．ゆえに

$$[(a+1)/b]\cdot b+\mathrm{rm}\,(a+1,b)=[a/b]\cdot b+\mathrm{rm}\,(a,b)+1=a+1$$

となって証明が完了した．

定理 35

$$c_1\cdot b+d_1=c_2\cdot b+d_2,\ d_1<b,\ d_2<b \rightarrow c_1=c_2\wedge d_1=d_2$$

(証明)　$c_1<c_2$　か　$c_2<c_1$　ならば矛盾することをいう．どちらでも同じであるから，　$c_2<c_1$

とすれば　$c_2\cdot b+d_2<c_2\cdot b+b=(c_2+1)\cdot b\leqslant c_1\cdot b\leqslant c_1\cdot b+d_1$

となって矛盾する．ゆえに　$c_1=c_2$.

これから　$d_1=d_2$

はただちにでる．

この定理の系としてつぎの定理はただちにでる．

定理 36　$a=c\cdot b+d\wedge d<b \rightarrow c=[a/b]\wedge d=\mathrm{rm}\,(a,b)$

さらにこの定理の系として

定理 37　$\mathrm{rm}\,(a+b\cdot c, b)=\mathrm{rm}\,(a,b)$

(証明)
$$a+b\cdot c=[a/b]\cdot b+\mathrm{rm}\,(a,b)+b\cdot c$$
$$=([a/b]+c)\cdot b+\mathrm{rm}\,(a,b)$$

ここで定理 36 を適用すればよい．

これでだいたい四則大小については自由自在に常識通りに行動してよいことがわかった．こんどは少し高級なことを考えることにしてよくでてくる $\sum$ について考えることにしよう．まず $f(a_1,\cdots,a_n,b)$ がすでにあたえられている関数であるとして

$$\sum_{b<c} f(a_1,\cdots,a_n,b)$$

を定義することを考えよう．

定義 12
$$\sum_{b<0} f(a_1,\cdots,a_n,b)=0$$
$$\sum_{b<c+1} f(a_1,\cdots,a_n,b)=f(a_1,\cdots,a_n,c)+\sum_{b<c} f(a_1,\cdots,a_n,b)$$

と定義する．

$\sum_{b<0} f(a_1,\cdots,a_n,b)$ は普通用いない記号なので変に感じるが，意味を考えてみると加えるべき項が 1 つもないのだから 0 とおくのは当然であろう．

$\sum_{b<c+1} f(a_1,\cdots,a_n,b)$ の意味は，もちろん

$$f(a_1,\cdots,a_n,0)+f(a_1,\cdots,a_n,1)+\cdots+f(a_1,\cdots,a_n,c)$$

である．

このほかに $\sum$ で $\sum_{y\leqq z}$ とか $\sum_{y=w}^{z}$ とか，いろいろな記号があって，それを全部ここで定義するわけにはいかないが，だいたいの考えを示すためにそのいくつかを書くと

$$\sum_{b\leqq c} f(b)=\sum_{b=0}^{c} f(b)=\sum_{b<c+1} f(b)$$

$$\sum_{a<b<c} f(b) = \sum_{b<c\dot{-}(a+1)} f(b+(a+1))$$

$$\sum_{a\leqq b\leqq c} f(b) = \sum_{b=a}^{c} f(b) = \sum_{b<(c+1)\dot{-}a} f(b+a)$$

となって，ここでいつでも一番左の式を右の式で定義すると思うのである．

論理との関係

さてわれわれの体系で定義されている命題 $P(a_1,\cdots,a_n)$ があたえられているとき，われわれの体系で定義されている関数 f があって，

$$P(a_1,\cdots,a_n) \leftrightarrow f(a_1,\cdots,a_n)=0$$

$$\rightarrow P(a_1,\cdots,a_n) \leftrightarrow f(a_1,\cdots,a_n)=1$$

なる 2 条件がみたされるとき，f は P の representing function であるといい，ここでは

repr. f.

と略記することにする．repr. f. はつねに 0 か 1 の値しかとらない．

われわれの体系の 1 つの特色は，この体系のなかからどんな命題 P をとってきても，われわれの体系のなかで定義された関数 f をとってきて，f が P の repr. f. であるようにできるということである．これを順々にやっていくことにしよう．

まず $a=b$ の repr. f. は何であろうか？　これは $\mathrm{sg}|a-b|$ である．定理の形にすれば，

定理 38

1)　$$a=b \leftrightarrow \mathrm{sg}|a-b|=0$$

2)　$$a\neq b \leftrightarrow \mathrm{sg}|a-b|=1$$

証明は簡単だから省略する．

つぎにわれわれの体系では，A と B とが命題であれば，$\rightarrow A$，$A\wedge B$，$A\vee B$，$A \rightarrow B$ も命題であるから，

$P(a_1,\cdots,a_n)$，$Q(a_1,\cdots,a_n)$ の repr. f.

がそれぞれ

$$f(a_1,\cdots,a_n),\quad g(a_1,\cdots,a_n)$$

であることを仮定して，

$$\neg P(a_1, \cdots, a_n),$$

$$P(a_1, \cdots, a_n) \vee Q(a_1, \cdots, a_n),$$

$$P(a_1, \cdots, a_n) \wedge Q(a_1, \cdots, a_n),$$

$$P(a_1, \cdots, a_n) \rightarrow Q(a_1, \cdots, a_n)$$

の repr. f. を求めることを考えねばならない.

ところで $P \wedge Q$ は $\neg(\neg P \vee \neg Q)$ と考えてよいし，$P \rightarrow Q$ は $\neg P \vee Q$ と考えてよい．ゆえに最初の 2 つだけを考えればよい．答は簡単で $\overline{\mathrm{sg}}(f(a_1, \cdots, a_n))$ と $f(a_1, \cdots, a_n) \cdot g(a_1, \cdots, a_n)$ である．定理の形にすれば，

定理 39　$f(a_1, \cdots, a_n)$ と $g(a_1, \cdots, a_n)$ がそれぞれ $P(a_1, \cdots, a_n)$，$Q(a_1, \cdots, a_n)$ の repr. f. であるとき

$$\overline{\mathrm{sg}}(f(a_1, \cdots, a_n)) \quad \text{および} \quad f(a_1, \cdots, a_n) \cdot g(a_1, \cdots, a_n)$$

の値はつねに 0 か 1 であって

$$\neg P(a_1, \cdots, a_n) \leftrightarrow \overline{\mathrm{sg}}(f(a_1, \cdots, a_n)) = 0$$

$$P(a_1, \cdots, a_n) \vee Q(a_1, \cdots, a_n) \leftrightarrow f(a_1, \cdots, a_n) \cdot g(a_1, \cdots, a_n) = 0$$

が成立する.

証明は簡単であるから省略する.

以上を組み合わせるとつぎの定理ができる.

定理 40　われわれの体系における勝手な命題 $P(a_1, \cdots, a_n)$ をとったとき，われわれの体系で定義された関数 f をとってきて，その値はつねに 0 か 1 であって

$$P(a_1, \cdots, a_n) \leftrightarrow f(a_1, \cdots, a_n) = 0$$

がつねに成立するようにできる.

証明は $P(a_1, \cdots, a_n)$ の構成に従って証明していけばよい.

$$P(a_1, \cdots, a_n) \quad \text{が} \quad s = t$$

の形であるときは，s と t のなかにたくさん関数が入っているかもしれないが，とにかく

$$\mathrm{sg}|s - t|$$

という関数を作ればよい．あとは定理 39 を用いればよいのである．

さて前に $\sum$ の定義をしたが，まだ $\prod$ の定義はしていない．$\sum$ の定義をして $\prod$ の定義をしないのは片手落である．$\sum$ のときと同様であるから，定義とはあらたまらないでここに書くことにすれば

$$\prod_{b<0} f(a_1, \cdots, a_n, b) = 1$$

$$\prod_{b<c+1} f(a_1, \cdots, a_n, b) = f(a_1, \cdots, a_n, c) \cdot \prod_{b<c} f(a_1, \cdots, a_n, b)$$

となる．

いま $f(a_1, \cdots, a_n, b)$ を $P(a_1, \cdots, a_n, b)$ の repr. f. とすると，$\prod_{b<c} f(a_1, \cdots, a_n, b)$ の意味は面白い．

これを見るために，最初に $\prod_{b<c} f(a_1, \cdots, a_n, b)$ の値がつねに 0 か 1 であることに注意して

$$\prod_{b<c} f(a_1, \cdots, a_n, b) = 0$$

になるのはどんなときか考えてみよう．

まず

$$c = 0$$

のときは，これは絶対に成立しない．

つぎに

$$c = 1$$

のときは

$$\prod_{b<1} f(a_1, \cdots, a_n, b) = f(a_1, \cdots, a_n, 0) \cdot 1 = 0$$

を意味するから

$$P(a_1, \cdots, a_n, 0)$$

を意味する．

さらに $c+1$ のときを考えると

$$\prod_{b<c+1} f(a_1, \cdots, a_n, b) = f(a_1, \cdots, a_n, c) \cdot \prod_{b<c} f(a_1, \cdots, a_n, b) = 0$$

となるから，これは

$$f(a_1, \cdots, a_n, c) = 0 \vee \prod_{b<c} f(a_1, \cdots, a_n, b) = 0$$

を意味する．すなわち

$$P(a_1, \cdots, a_n, c) \vee \prod_{b<c} f(a_1, \cdots, a_n, b) = 0$$

を意味する．順々にやってみると

$$\prod_{b<c+1} f(a_1, \cdots, a_n, b)=0$$

は実際には

$$P(a_1, \cdots, a_n, 0) \vee P(a_1, \cdots, a_n, 1) \vee \cdots \vee P(a_1, \cdots, a_n, c)$$

を意味することがわかる．これは $b<c+1$ なる b で $P(a_1, \cdots, a_n, b)$ をみたすものが存在するということである．ゆえにわれわれは

$$\exists x<c\, P(a_1, \cdots a_n, x)$$

を

$$\prod_{x<c} f(a_1, \cdots, a_n, x)=0$$

という式で定義することにする．ここで $\exists$ を用いたが，これはわれわれの体系のなかで完全に定義したのであるから，われわれの平和憲法に違反していないことに注意してほしい．もちろん形は似ていても $\exists x P(a_1, \cdots, a_n, x)$ 自身はわれわれの体系のなかで定義することはできない．$\exists x<c\, P(a_1, \cdots, a_n, x)$ が定義できるということはじつはこれは

$$P(a_1 \cdots, a_n, 0),\ P(a_1, \cdots, a_n, 1), \cdots$$

と順々に c に至るまで調べてみれば完全にわかることであるから，もともとわれわれの体系の精神に従ったもので，よってこれから定義されることはむしろ当然というべきであろう．

定理 41　　$b<c \wedge P(a_1, \cdots, a_n, b) \rightarrow \exists x<c\, P(a_1, \cdots, a_n, x)$

（証明）　　$f(a_1, \cdots, a_n, b)=0, b<c \rightarrow \prod_{x<c} f(a_1, \cdots, a_n, x)=0$

をいえばよい．これは c についての帰納法で簡単に証明される．

定理 42　　$b<c \wedge P(a_1, \cdots, a_n, b) \rightarrow Q(a_1, \cdots, a_n, c)$

がつねに成立しており，変数 b は $P(a_1, \cdots, a_n, a), Q(a_1, \cdots, a_n, a)$ のなかに含まれていないとする：そのとき

$$\exists x<c\, P(a_1, \cdots, a_n, x) \rightarrow Q(a_1, \cdots, a_n, c)$$

が成立する．

（証明）　　$d \leqq c \wedge \exists x<d\, P(a_1, \cdots, a_n, x) \rightarrow Q(a_1, \cdots, a_n, c)$

を d についての帰納法で証明する．

大筋を書くと，
$$d=0$$
のときは
$$\exists x < d\, P(a_1, \cdots, a_n, x) \text{ は偽}$$
であるから明らかである．いま
$$d=b+1 \text{ で } d \leqslant c$$
であるとすると
$$\begin{aligned}&\exists x < d\, P(a_1, \cdots, a_n, x)\\ &\to P(a_1, \cdots, a_n, b) \vee \exists x < b P(a_1, \cdots, a_n, x)\\ &\to P(a_1, \cdots, a_n, b) \vee Q(a_1, \cdots, a_n, c)\\ &\to Q(a_1, \cdots, a_n, c)\end{aligned}$$
となって証明が完了する．

いま
$$\forall x < c\, P(a_1, \cdots, a_n, x)$$
のことを
$$\neg \exists x < c \neg P(a_1, \cdots, a_n, x)$$
と定義すれば，定理 41 と 42 から明らかにつぎの 2 定理がでる．

定理 43 $\quad b < c \wedge \forall x < c\, P(a_1, \cdots, a_n, x) \to P(a_1, \cdots, a_n, b)$

定理 44 $\quad b < c \wedge Q(a_1, \cdots, a_n, c) \to P(a_1, \cdots, a_n, b)$

がつねに成立しており，変数 b は $P(a_1, \cdots, a_n, a)$，$Q(a_1, \cdots, a_n, a)$ のなかに含まれていないとする．そのとき
$$Q(a_1, \cdots, a_n, c) \to \forall x < c\, P(a_1, \cdots, a_n, x)$$
が成立する．

定義 13 $f(a_1, \cdots, a_n, b)$ を $R(a_1, \cdots, a_n, b)$ の repr. f. とするとき，
$$\mu y < c\, R(a_1, \cdots, a_n, y)$$
を
$$\sum_{y<c} \prod_{x \leqslant y} f(a_1, \cdots, a_n, x)$$
によって定義する．くわしくいえば
$$g(a_1, \cdots, a_n, y) = \prod_{x \leqslant y} f(a_1, \cdots, a_n, x)$$
と定義したうえで
$$\mu y < c\, R(a_1, \cdots, a_n, y) = \sum_{y<c} g(a_1, \cdots, a_n, y)$$

と定義するのである．

じつはこの $\mu y < c\, R(a_1, \cdots, a_n, y)$ は $y < c$ で $R(a_1, \cdots, a_n, y)$ をみたすものがあれば，その最小の y，またそのような y が 1 つもなければ c と定義したものになっているが，そのことを証明していこう．以下面倒だから $R(a_1, \cdots, a_n, y)$ を単に $R(y)$ と書くことにして $R(y)$ の repr.f. を $f(y)$ としよう．

定理 45　$\neg \exists y < c\, R(y) \rightarrow \mu y < c\, R(y) = c$

（証明）　まず

$$\neg \exists y < c\, R(y), \quad b < c \rightarrow f(b) = 1$$

あとは
$$d < c \rightarrow g(d) = 1$$
を d についての帰納法で，またそのあとで
$$d \leqq c \rightarrow \mu y < d\, R(y) = d$$
を d についての帰納法で証明すればよい．

定理 46　$\mu y < c\, R(y) \leqq c$

（証明）　これは c についての帰納法で，簡単に証明できる．

定理 47　$b < c \wedge R(b) \rightarrow \mu y < c\, R(y) \leqq b$

（証明）
$$f(b) = 0$$
だから d についての帰納法で
$$b \leqq d \rightarrow \prod_{x \leqq d} f(x) = 0$$
ゆえにふたたび d についての帰納法で
$$b \leqq d \rightarrow \sum_{y < d} \prod_{x \leqq y} f(x) = \sum_{y < b} \prod_{x \leqq y} f(x)$$
がいえて定理 46 より証明される．

定理 48　$a = \mu y < c\, R(y) \wedge \exists y < c\, R(y) \rightarrow R(a)$

（証明）　定理 42 によって
$$b < c \wedge R(b) \wedge a = \mu y < c\, R(y) \rightarrow R(a)$$
をいえばよい．まず定理 47 により
$$a \leqq b < c$$

である．またいま　$x<a$

とすれば，　$x<c$

であるから定理 47 により　$\neg R(x)$.

すなわち　$f(x)=1$

となる．ゆえに　$\mu y<d\,R(y)=d$

が $d\leqq a$ なる仮定のもとでの d についての帰納法で証明される．ゆえに

$$\mu y<aR(y)=a$$

また，もし　$\neg R(a)$ すなわち $f(a)=1$

とすれば　$\mu y<a+1\,R(y)=a+1$

となり　$\mu y<a+1\,R(y)\leqq\mu y<c\,R(y)$

は明らかであるから　矛盾する．

ついでにもう 1 つだけ大切なことをのべておこう．

いま $Q_1(a_1,\cdots,a_n),\cdots,\ Q_m(a_1,\cdots,a_n)$ が互いに交わらない，というのは $i<j\leqq m$ なる i,j を勝手にとってきたとき，つねに

$$\neg(Q_i(a_1,\cdots,a_n)\wedge Q_j(a_1,\cdots,a_n))$$

が成立することと考えることにする．

いま互いに交わらない $Q_1,\ \cdots,\ Q_m$，すでにあたえられている関数 $f_1,\cdots,f_m,f_{m+1}$ があるときに，新しい関数 f をつぎのように定義することは，よく行なわれるが，それがわれわれの体系のなかでも実行できるということである．

$$f(a_1,\cdots,a_n)=\begin{cases} f_1(a_1,\cdots,a_n) & Q_1(a_1,\cdots,a_n)\ \text{のとき} \\ \quad\vdots & \\ f_m(a_1,\cdots,a_n) & Q_m(a_1,\cdots,a_n)\ \text{のとき} \\ f_{m+1}(a_1,\cdots,a_n) & \text{上のどれでもないとき} \end{cases}$$

実際には $Q_1,\cdots,Q_m$ の repr. f. をそれぞれ，$g_1,\cdots,g_m$ として

$$f=\overline{\mathrm{sg}}(g_1)\cdot f_1+\cdots+\overline{\mathrm{sg}}(g_m)\cdot f_m+g_1\cdots\cdot g_m\cdot f_{m+1}$$

と定義すればよいのである．これが上の性質をみたすことは簡単なので演習問題としておく．

素数について

だいぶ論理との関係に深入りをしてしまったが，整数論の入口といえばやはり素数の定義をして，素因数分解の一意性を証明するということになるだろう．遅ればせながら，そのことについて考えてみることにする．

定義 14　'a が b を割る' ということを

$$a|b$$

と書いて，

$$\exists x \leqslant b(ax=b)$$

によって定義する．

$\exists x \leqslant b$ は厳密には $\exists x < (b+1)$ であって，すでにわれわれの体系で用いてよいことが判明しているわけである．

定義からただちにわかる性質としてつぎのものがある．

定理 49

1)　$a|0$

2)　$0|a \rightarrow a=0$

3)　$a|a \cdot b$

4)　$a|b \rightarrow a|b \cdot c$

5)　$1|a$

6)　$a|1 \rightarrow a=1$

この定理から $a|b$ は $a>1$ で $b>1$ のとき以外はあまり意味がないことがわかる．

定義 15　'a が素数である' ということを

$$\mathrm{Pr}(a)$$

で表わして

$$a>1 \wedge \forall x < a \rightarrow (1<x \wedge x|a)$$

によって定義をする．

この定義から明らかなこととして

定理 50

1)　$$\mathrm{Pr}(2)\wedge\mathrm{Pr}(3)$$

2)　$$\mathrm{Pr}(a)\wedge b|a \ \rightarrow\ b=a\vee b=1$$

3)　$$a>1\wedge b>1 \ \rightarrow\ \neg\mathrm{Pr}(a\cdot b)$$

定義 16

$$0!=1$$

$$(a+1)!=(a+1)\cdot a!$$

これはよく知られた $a!$ の定義である．

簡単な性質として

定理 51　$$0<b\leqq a \ \rightarrow\ b|a!$$

いま $\neg(a|b)$ を

$$a\not| b$$

と表わすことにすれば

定理 52　$$a>1\wedge a|b \ \rightarrow\ a\not|(b+1)$$

(証明)　$$a|b$$

ならば　$b=[b/a]\cdot a$ で $\mathrm{rm}(b,a)=0$

である．ところで

$$\mathrm{rm}\,(b+1,a)=\mathrm{rm}\,([b/a]\cdot a+1,a)$$
$$=\mathrm{rm}\,(1,a)$$
$$=1 \qquad (a>1\ \text{だから})$$

ところで　$$a|(b+1)$$

ならば，　$$\mathrm{rm}\,(b+1,a)=0$$

となるから　矛盾する．

定理 53　$$\exists x<a!+2(a<x\wedge\mathrm{Pr}(x))$$

(証明)　$$\forall x<a!+2(a<x\ \rightarrow\ \neg\mathrm{Pr}(x))$$

を仮定して矛盾をだせばよい．いま $a!+1$ を考えると明らかにこれは a より大きい．また定理 51 と 52 とによって

$$\forall x\leqq a(1<x\ \rightarrow\ x\not|(a!+1))$$

をみたす．いま　$b=\mu y<a!+2(\forall x\leqq a(1<x\ \rightarrow\ x\not| y)\wedge a<y)$

とおけば，b は

$$\forall x \leqslant a(1<x \rightarrow x \nmid b) \wedge a<b$$

なる b の最小なものであり，したがって

$$b \leqslant a!+1$$

となる．ところで仮定により　$\rightarrow \mathrm{Pr}(b)$

であるから，　$x>1$ で $x|b$

なるものがある．ところで　$x<b$

であるから，b の最小性によって

$$\exists y \leqslant a(1<y \wedge y \mid x)$$

となる．この y をとれば，

$y|b$ となって矛盾する．

この定理によって i 番目の素数というのを定義することができる．すなわち 0 番目の素数を 2，1 番目の素数を 3 というふうに定義していって 'i 番目の素数' を p_i と表わすことにすれば

定義 17

$$p_0=2$$

$$p_{i+1}=\mu x< p_i!+2\ (p_i<x \wedge \mathrm{Pr}(x))$$

前定理より明らかなのは

定理 54

1) $\mathrm{Pr}(p_i)$

2) $p_i<b \wedge \mathrm{Pr}(b) \rightarrow p_{i+1} \leqslant b$

3) $i<p_i$

4) $\mathrm{Pr}(b) \wedge i=\mu j<b+1(p_j \geqslant b) \rightarrow b=p_i$

（証明） 1)，2) は定義より明らか．3) は i についての帰納法より明らか．4) は 3) を用いて最小性の性質から容易にでてくる．

思ったより意外に手間どってしまって，素数を並べたところで今回の紙数がつきてしまった．つぎにはもう少しだけ整数論を展開して，そのうえでわ

れわれの体系について，いったい何をやっているのか？　また，この体系についての未解決の問題は何であるかを証明することにしたい．

素因数分解

前節でやっと素数が無限にあることをのべた．いまからおもむろに素因数分解についてのべることにする．考えてみると，整数論については近くは正田建次郎先生，また以前に遠山啓先生の名講義が『数学セミナー』にあって同じようなことをここでのべるのはあまり意味がないように思われるが，文明から離れて孤島の生活をしてみようという物好きからはじまった話であるから，その点ご了解を願いたい．正田先生のも遠山先生のも文明の利器をやさしくわかり易く話されているが，ここでは逆に非文明の不自由さを楽しもうというのである．しかしながら，いずれにしても中味はもうここまでくれば，それほどの差はない．どうせのことに一段落つくまでのところをキチンと見極めようということである．

定義 18　　$b|c$ で $a|c$

であるとき，c を a,b の**公倍数**という．$a \cdot b$ が a,b の公倍数であることはたしかであるから，a,b の**最小公倍数**は

$$\mu x < a \cdot b + 1 (a|x \wedge b|x \wedge 0 < x)$$

としてキチンと定義される．

ここにきて思い出したが，$a|b$ のとき，b を a の**倍数**，a を b の**約数**というのである．こういう定義はほかにも忘れて用いたかもしれないが，理解のさまたげにならなかったことを希望する．

さていま a が b の約数であり，また c の約数であるとき a は b と c との**公約数**というのであるが，

a が b と c との公約数

として　　$c \leqslant b$

であったとする．このとき

$$b=[b/a]\cdot a$$

$$c=[c/a]\cdot a$$

で

$$[c/a]\leqslant[b/a]$$

となる．ゆえに

$$b\dot{-}c=([b/a]\dot{-}[c/a])\cdot a$$

となる．これから a は $b\dot{-}c$ の約数であることがわかる．さらに

$$b=[b/c]\cdot c+\mathrm{rm}\,(b,c)$$

で

$$a|b$$

また

$$a|[b/c]\cdot c$$

であるから，いまいったことから

$$a|\mathrm{rm}\,(b,c)$$

がわかる．

定理 55　a を b,c の最小公倍数とし，d を b,c の公倍数とするとき $a|d$.

(証明)

$$b|\mathrm{rm}\,(d,a),\ \ c|\mathrm{rm}\,(d,a)$$

であるから　$\mathrm{rm}\,(d,a)$ は b,c の公倍数.

ところで，

$$\mathrm{rm}\,(d,a)<a.$$

ゆえに

$$\mathrm{rm}\,(d,a)=0,$$

すなわち

$$a|d.$$

最小公倍数の理論は簡単だが最大公約数の理論はあまり簡単ではない．第1にわれわれの体系ではキチンと定義すると少しゴタゴタして気持が悪い．いま a,b をとってきて $\min(a,b)>0$ であるとしよう．a,b の最大公約数を表わすためには，公約数はすでに表わされているから，最大だけを表わすことができればよい．いま最大公約数を x として

$$y=\min(a,b)\dot{-}x$$

とおけば $x=\min(a,b)\dot{-}y$ となるから y を表わせばよい．x における最大の条件は y においては最小の条件になるから，これは

$$\mu y<\min(a,b)+1$$

を用いて簡単に表わすことができる．もちろんこうして最大公約数の存在を

いうためには，少なくとも1つ公約数が存在することを使わなければならないが，これは1が公約数となるから心配はいらない．ここに以上のキチンとした定義は書かないが，こうして関数の形に表わされた a,b の最大公約数を

$$(a,b)$$

と書くことにする．(a,b) はわれわれの体系のなかの関数になっていることが大切である．

つぎに少し複雑な帰納法をやるための準備をしておこう．

定理 56　$P(a)$ がわれわれの体系のなかで定義された命題で

$$\forall x<a\, P(x) \rightarrow P(a)$$

がつねに成立しているとき，$P(a)$ はつねに成立する．ここに $\forall x<a\, P(x)$ という $\forall$ が入っている命題を書いたが，これは省略記号で全部キチンとわれわれの体系のなかで定義できることを思い出してほしい．

(証明)　$\neg P(a)$ を仮定して矛盾を導けばよい．いま

$$\neg P(a)$$

として　　$b=\mu x<a+1\, \neg P(x)$

とおけば　　$\neg P(b)$

また　　b の最小性

から　　$\forall x<b\, P(x)$

したがって仮定から　　$P(b)$

となって　　矛盾する．

定理 57　a,b を正で，c を a,b の公約数とするとき $c|(a,b)$．

(証明)　$r=\min(a,b)$ についての定理 56 の形の帰納法で証明する．(われわれの体系でのキチンとした表現は演習問題としたい．)

$$a=b$$

とすれば定理は当然であるから，いま

$$a<b$$

とする．このとき　a,b の公約数は $a, \mathrm{rm}(b,a)$ の公約数

である．ゆえに　　$(a,b)=(a,\mathrm{rm}(b,a))$．

ところで　$\min(a, \mathrm{rm}(b, a)) = \mathrm{rm}(b, a) < a = \min(a, b)$

であるから，帰納法の仮定により

$$c \mid (a, b)$$

がいえた．

定理 58　$(ma, mb) = m(a, b)$

(証明)　$m(a, b) \mid ma, \quad m(a, b) \mid mb$

は明らかだから　$m(a, b) \mid (ma, mb)$

が定理 57 よりでる．

逆に　$d' = (ma, mb)$

とすれば，　m は ma, mb の公約数

であるから定理 57 により，　$m \mid d'$

となる．

いま　$d' = m \cdot d_0'$

とすれば，(もしウルサイことをいえば $d_0' \leqq d'$ と考えてよいから d_0' はわれわれの体系のなかでキチンと定義することができる.)

$$m \cdot d_0' \mid ma, \quad m \cdot d_0' \mid mb$$

から　$d_0' \mid a, \quad d_0' \mid b$

がでて　d_0' は a, b の公約数，

すなわち　$d_0' \mid (a, b)$

がいえて　$(ma, mb) \mid m(a, b)$

がわかった．

定理 59　m を a, b の最小公倍数，$d = (a, b)$ とするとき，$md = ab$.

(証明)　$a = a_0 d, \quad b = b_0 d$

とすれば，明らかに　$(a_0, b_0) = 1$　(定理 58)

ゆえに　$(ma_0, mb_0) = m$　(定理 58)

したがって　$a_0 b_0 d \mid ma_0, \quad a_0 b_0 d \mid mb_0$

から　$a_0 b_0 d \mid m$

また逆に　$a \mid a_0 b_0 d, \quad b \mid a_0 b_0 d$

から　　$m|a_0b_0d$

ゆえに　　$a_0b_0d=m$

したがって　　$a\cdot b=m\cdot d$

定理 60　　$(a,b)=1 \to (ac,b)=(c,b)$

(証明)　　$(ac,b)|(ac,bc)=c$

は明らかだから　　$(ac,b)|b$

から　　$(ac,b)|(c,b)$

がでる．

逆に　　$(c,b)|(ac,b)$

は明らかである．

定理 61　　$(a,b)=1,(a,c)=1 \to (a,bc)=1$

(証明)　定理 60 より　　$(a,b)=1$

から　　$(bc,a)=(c,a)=1$

定理 62　　$(a,b)=1, a|bc \to a|c$

(証明)　　$(a,c)=(bc,a)=a$

ゆえに　　$a|c.$

定理 63　　$\mathrm{Pr}(p), p|bc \to p|b \vee p|c$

(証明)　p の因数は 1 と p しかないから

$$p \nmid b$$

ならば　　$(p,b)=1.$

いま　　$(p,b)=1,\quad (p,c)=1$

とすれば　　$(p,bc)=1$

となって　　$p|bc$ に矛盾する．

ここまでくると，素因数分解の一意性の証明にあまりかわったことはないから，あまり細部にはこだわらないことにしよう．

定理 64　　$a>1 \to \exists x<a+1(\mathrm{Pr}(x) \wedge x|a)$

(証明)　定理 56 の形の帰納法を用いればよい．

定義 19　　$(a)_i = \mu x < a(p_i{}^x | a \wedge p_i{}^{x+1} \nmid a)$

すなわち $(a)_i$ は p_i の x ベキが，ちょうど a の因数になっているような最大の x のことである．

いま $(a, b)=1$ のことを 'a と b とは互いに素' ということにすれば，

$$i \neq j \text{ のとき } (p_i, p_j)=1$$

は明らかである．ゆえに簡単に　$(p_i{}^a, p_j{}^b)=1$

がでてくる．

いま　$p_i{}^a | c, \quad p_j{}^b | c$

とすれば　$c = c_0 \cdot p_j{}^b$

として　$(p_i{}^a, c_0) = (p_i{}^a, c_0 \cdot p_j{}^b) = (p_i{}^a, c) = p_i{}^a$

だから　$(p_i{}^a p_j{}^b, c) = p_j{}^b (p_i{}^a, c_0) = p_j{}^b \cdot p_i{}^a$

となる．

ゆえに一般に，　$p_0{}^{a_0} | c, \ \cdots, \ p_n{}^{a_n} | c$

ならば　$p_0{}^{a_0} \cdot \cdots \cdot p_n{}^{a_n} | c$

がいえる．

この論法によって

$$\prod_{i<a+1} p_i{}^{(a)_i} = p_0{}^{(a)_0} p_1{}^{(a)_1} \cdots p_a{}^{(a)_a}$$

を考えると　$\prod_{i<a+1} p_i{}^{(a)_i} | a$

がいえる．いまもし $(\prod_{i<a+1} p_i{}^{(a)_i}) \cdot d = a$ である $d > 1$ があるとして d の素因数 p が存在するとすれば，$p \leqq a$ から $p = p_i$ なる $i < a+1$ が存在する．これは $(a)_i$ の定義に反する．したがって

$$\prod_{i<a+1} p_i{}^{(a)_i} = a$$

が証明されたことになる．このあたりはやや省略したが，だいたいわれわれの体系のなかでこのような議論がとどこおりなく進行することは見当がつかれることと思う．

あとの議論のために必要なこととして，ちょっとした定義をすることにする．

定義 20　あたえられた関数 f について

$$\tilde{f}(y, x_2, \cdots, x_n) = \prod_{i<y} p_i^{f(i, x_2, \cdots, x_n)}$$

で定義される関数を course-of-values function といって

c. o. v. f.

と略記することにする．

定理 65　g がわれわれの体系のなかの関数であるとき，

$$f(y, x_2, \cdots, x_n) = g(y, \tilde{f}(y, x_2, \cdots, x_n), x_2, \cdots, x_n)$$

をみたす関数 f がわれわれの体系のなかに存在する．ここに $\tilde{f}$ は f の c. o. v. f. である．

（証明）　最初に $\tilde{f}$ を（f の c. o. v. f. だとは考えないで）

$$\tilde{f}(0, x_2, \cdots, x_n) = 1$$

$$\tilde{f}(y+1, x_2, \cdots, x_n) = \tilde{f}(y, x_2, \cdots, x_n) \cdot p_y^{g(y, \tilde{f}(y, x_2, \cdots, x_n), x_2, \cdots, x_n)}$$

というわれわれの体系で許された方法で定義して，それから

$$f(y, x_2, \cdots, x_n) = (\tilde{f}(y+1, x_2, \cdots, x_n))_y$$

によって f を定義すれば f が定理をみたすことは明らかである．

数学基礎論の立場から

いままで「初等初等整数論」と銘を打って長い間お付合いを願ってきたが，いったいわれわれのやっていることはどんなことなのであろうか？

じつは，いままでのべてきた体系は，数学基礎論でいう quantifier free primitive recursive arithmetic というものなのである．これは長すぎるから q. f. p. r. a. と略記することにする．さてそれでは q. f. p. r. a. はどのような意味で数学基礎論で考えてこられているのであろうか？

少しあとで有限の立場についてのべてみるが，有限の立場のなかに 2 通りあるように感じられる．1 つはこの本でとりあげるように数列があたえられたときに，その数列についての有限的考察をするという，やや高級な立場である．もちろんこの本で論じようとするのは，そのような高級なものを

選んで論じるのであるが，有限の立場の多くの推論はもっと素朴な純粋なものである．ここではそれを狭義の有限の立場と呼ぶことにしよう．狭義の有限の立場における，いろいろな展開および推論は，たとえば，小著

『数学基礎論』共立出版

に多く見られるから，それらによっていろいろ判断していただきたい．ところで狭義の有限の立場というものを形式化すればどうなるであろうか？　その答の 1 つの可能性がいままでのべてきた q.f.p.r.a. なのである．まずハッキリいえることは q.f.p.r.a. で行なわれることはすべて狭義の有限の立場に入っているといってさしつかえないということである．

問題は逆である．逆ははたして正しいであろうか？　すべての狭義の有限の立場の議論は q.f.p.r.a. のなかで翻訳可能と思ってよいであろうか？

もちろん狭義の有限の立場にハッキリとした定義があるわけではないから，これは証明することも，反証することもできない類の問題である．しかしながら今日多くの専門家がこれを信じて疑わないようである．

しかしながら正直にいうと，私はこの考えには大きな疑問をいだかずにはいられない．まず私なりの意見をのべることにすると，よく知られたユークリッドの互除法を考えてみよう．この操作が有限の立場で定義されそれが有限回で完了する手続きであることは，多少有限の立場になじんだ人にとっては明白なことであろう．ところでこれを q.f.p.r.a. でやろうとすると，どうなるであろうか？

なかなかうまくはできないのである．その理由はやってみようとすれば明白だが，うまくできないという以上には説明しがたい．しかしこの本で，互除法に相当するところでだいぶ手こずっているのをもう一度冷やかに観察されればその間の苦情はやや見当がつかれるかもしれない．

もちろんこの互除法に相当するものが q.f.p.r.a. で絶対にできないというのではない．先ほどのべた定理の方法を用いれば遂行できるのである．しかしこれは考えてみれば妙な話である．普通ユークリッドの互除法は素因数分解の一意性を証明するための基礎的な事項として用いるのである．ここで

はそれらを総動員してユークリッドの互除法に相当することをやるのである．この例は絶対的とはいえないが，狭義の有限の立場と q.f.p.r.a. との間にかなりの相対的な差があることを示しているように思われる．だからもし初等整数論を q.f.p.r.a. の体系においてかなり調べていけば，q.f.p.r.a. では証明できなくて狭義の有限の立場ではなるほどできるとみんながウナズクような例が見つからないかと思うのだが，どんなものだろうか？　このプログラムが実際にはなかなかむずかしいことは，またもう少しあとで説明することにする．

つぎに初等整数論の定理は全部 q.f.p.r.a. で証明できるのか？という問題である．もちろん初等整数論には $\forall x$ か $\exists y$ をふんだんに用いた定理があるからこういう定理は q.f.p.r.a. では証明はおろか書くことすらできない．だからもちろん初等整数論の定理で

$$P(a_1, \cdots, a_n)$$

がつねに正しいという形で $P(a_1, \cdots, a_n)$ が q.f.p.r.a. の命題であるようなものはつねに q.f.r.p.a. で証明ができるか？という問題である．これは現在の初等整数論に限って考えると，未解決のきわめて面白い問題である．誰かがよく知られた整数論の定理で q.f.p.r.a. で書けるが証明できないということを証明すれば，ちょっとした評判になるであろう．この問題には原理的な困難もあるが，それ以上にいままであまり誰もキチンと考えていないことがおもな原因であるように思われる．数学基礎論はいままで，一般論の展開がおもな関心事で，ほんとうの目的である数学を細かく調べ観察するという点ではどちらかといえば弱いのである．これからはそういうふうにも発展していくことを期待してやまない．

さて問題をもう少し一般的にして，q.f.p.r.a. で表現できる正しい定理で q.f.p.r.a. では証明できないものがあるか？と問い直せば，これはゲーデルの不完全性定理からただちに答がでてくる．

q.f.p.r.a. でも命題のゲーデル数というのを定義することができるし，これによって‘ある自然数 p が q.f.p.r.a. の証明のゲーデル数になっている’

というような概念や，さらに‘p が矛盾への q.f.p.r.a. での証明のゲーデル数になっている’という命題を q.f.p.r.a. の命題と定義することができる．後者をかりに $Q(p)$ とおくならば

$$\neg Q(a)$$

が求める定理である．この定理はしかも普通のペアノの算術の公理系のなかで証明することができるから基礎論の立場からいえばきわめて初等的な定理である．

もっともこういう基礎論的な命題までもっていかなくても，こういう命題があることは常識から見当がつく．たとえばフェルマーの大定理を考えてみよう．これは

$$2<n\wedge 0<x\wedge 0<y\wedge 0<z \rightarrow x^n+y^n\neq z^n$$

と q.f.p.r.a. のなかで表現可能である．q.f.p.r.a. はかなり弱い体系であるから，このような難定理が証明できようとはとても思えないという意見はマア妥当といってよいだろう．

ゴールドバッハの問題についてもそうである．

$$3<x \rightarrow \exists p<x+x\exists q<x+x(\mathrm{Pr}(p)\wedge\mathrm{Pr}(q)\wedge p+q=x+x)$$

として q.f.p.r.a. で表わすことができるのである．あまり楽観的な考えをもつといけないので一言注意しておくが，双子素数の問題は q.f.p.r.a. では表現することはできない．（したがって双子素数の問題はわれわれ人間の立場にとっては，真とか偽とかが意味のない問題である，という人がある．）

こう考えてみると，フェルマーの問題や，ゴールドバッハの問題が q.f.p.r.a. で証明できないことを証明するというのはきわめて実際的な問題であるように思われる．ところが考えてみると全然やさしくないのである．なぜであろうか？　じつはこの方面の数学基礎論は極度に未発達で何をしてよいのか見当もつかないのである．誤解を避けるためにいっておくが，これはフェルマーの問題やゴールドバッハの問題がむずかしいということと何の関係もない．問題がむずかしいほど，弱い体系で証明ができない証明はやさしいはずである．

さてこれだけのべたあとでは，以前に残しておいた，初等関数論の定理で q.f.p.r.a. で証明できないものを見つけるというのが困難であることはだいたい明らかになったかと思う．実際に初等整数論の定理を全部チェックしてこれは証明できそうもないというものを見つけることは恐らくは時間とエネルギーだけの問題であろうが，それが見つかったときに，それがほんとうに q.f.p.r.a. で証明できないということを証明するような手段は現在のところもち合わせがないのである．

つぎにこの方面の研究について大略をのべたい．この分野は A. Church とその弟子たち Guard, H.E. Rose 等によって熱心に研究された．そのほか Curry-Goodstein, Cleave-Rose, D. Richerdson, Shepherdson などの研究がある．しかし q.f.p.r.a. 自身の研究は驚くほど少ない．たいていは関数を 2 変数の関数に制限した場合，3 変数だけに制限した場合，＋, ×, exp. に制限した場合，＋，× だけに制限した場合というような変則な研究ばかりである．このなかで面白いのは Shepherdson の仕事で，彼は関数を ＋，× だけに制限した q.f.p.r.a. では

$$0<a \rightarrow 2a^2 \neq b^2$$

が証明できない，ということを証明した．

わずかに Guard だけが q.f.p.r.a. についての研究をしている．しかしこれも厳密にいってほんとうの意味での q.f.p.r.a. についてではない．彼は q.f.p.r.a. に命題についての自由変数を導入して，それによって，いろいろの線型順序 $\prec$ が整列であることが証明できることを q.f.p.r.a. で表現できるようにして，どのような線型順序について超限帰納法が証明でき，どのような線型順序についてはできないか？ を調べたのである．彼の定理は

$\alpha<\omega^\omega$ ならば，α までの超限帰納法は q.f.p.r.a. で証明でき，$\alpha\geqq\omega^\omega$ ならばできない．

というのである．これが厳密な意味で q.f.p.r.a. についてのよい定理といってよいであろう．

この小文の目的は，q.f.p.r.a. が数学基礎論入門のためにとてもよい分野であると信じていたからであるが，また一方において，少しこの方面を強調し認識を改めたかったからでもある．

初等整数論を数学基礎論の手段でキチンと調べ，研究するということは，現在の数学基礎論，とくに証明論にとっては有意義でもあり，またよい刺激でもあると思うのである．私自身はいつかおりがあったら本格的にやってみたいと思っているが未だ機会に恵まれない．*

計算できる関数について一言

さていわなければならないことは一通りいったから，もう少し基礎論の立場から常識的な用語を説明することにすると，われわれの体系で定義される関数のことを primitive recursive function（原始帰納関数）と呼んでいる．ここでは p.r.f. と略記する．いわゆる計算できる関数 recursive function（帰納的関数，ここでは r.f. と略記する）の全体は p.r.f. の全体につぎの操作をつけ加えて得られる関数の全体（くわしくいえば，この操作によって得られたものにもとからある関数と関数結合をして得られる関数の全体）をいうのである．

$f(x,y)$ から $\mu y f(x,y)$ を作る．

ただしここに

$\forall x \exists y(f(x,y)=0)$ がみたされているものとする．

ここで $\mu y f(x,y)$ とは $f(x,y)=0$ となるような最小の y のことである．

$f(x,y)$ が p.r.f. であって，$\forall x \exists y(f(x,y)=0)$ がみたされているときに $\mu y f(x,y)$ が計算できることは容易にわかる．すなわち $g(x)=\mu y f(x,y)$ とおけば

$f(x,0)$ を計算してみる．もしそれが 0 ならば，$g(x)=0$ である．

---

*　高橋元男氏の私信によれば，彼も同様なことに興味をもっているようである．遠方に朋あり，また楽しからず乎．

上の場合でないときは，$f(x,1)$ を計算してみる．もしその値が 0 ならば $g(x)=1$ である．

上のどの場合でもないときは，$f(x,2)$ を計算してみる．もしその値が 0 ならば $g(x)=2$ である．

……

この計算を $g(x)$ の値が確定するまで，いつまででもやっていくのである．この計算がいつかは終了するという保証がすなわち $\forall x \exists y(f(x,y)=0)$ という条件である．したがってこの条件 $\forall x \exists y(f(x,y)=0)$ がなければ $\mu y f(x,y)$ はいったい値がいつ求められるのか，それとも値がないのか全然見当がつかないから計算できる関数とはなりえない．

このように r.f. の定義は $\forall x \exists y(f(x,y)=0)$ というようなわれわれの体系に入らないような超越的な条件のうえで考えられているので，じつはきわめて超越的な考え方である．すなわち r.f. の理論を考えるときは集合論的な考えが基盤にあって，そのうえで考えているものといってよいであろう．これに反して p.r.f. はトコトンまでわかりうる，納得のいった世界の住人といってよいであろう．

ついでに r.f. の条件 $\forall x \exists y(f(x,y)=0)$ がみたされていない，またはみたされているかどうかわからないときでも

$$g(x)=\mu y(f(x,y))$$

を考えて，その定義は r.f. のときと同じように計算していく．もし値が求められたときにはそれは，$g(x)$ の値で，もしも値が求められないときにはただいつまでも計算を続行していく．そしてこのときは神のごとき超越的な立場では値は定義されないと定義することにする．

こういうふうに考えて拡張することもある．このように拡張した μy を導入してそれでできた partial function（すなわち値が全部定義できているとはかぎらない関数）にもとからある関数の関数結合をしてできた関数の全体を partially recursive function と呼ぶのである．

もちろんp.r.f. は r.f. であり，r.f. は partially r.f. である．

partially r.f. の関数結合

$$f(g(x))$$

で，もし $g(x)$ の値が定義されていないときは，$f(g(x))$ の値は定義されていないと考えるのである.

この r.f. および partially r.f. は計算機と密接な関係のあることは，いろいろなところで再々解説されるのでよくご存知のことと思う. partially r.f. の定義がされない個所はちょうど計算機がいつまでも動いていて stop しないところだと思えばよい.

文明の世を避けて孤島のロビンソン・クルーソーの生活を味わいたいとしてはじめた話も最後は計算機の話になってしまった. 御時世というものであろうか？

有限の立場について

有限の立場

純粋であろう，不純なものを避けよう．人間的であろう．自己に忠実であろう．できないものはできないとハッキリ認めよう．物事を想像で判断することをやめよう．ハッキリと確かめたこと以外は認めないことにしよう．

などといったら，何か人生修養の本の一節のようになるが，じつはこれは有限の立場のモットーを書いたのである．

現代数学のたいていの議論は有限の立場には入らないのであるが，まずその例をあげて，それから有限の立場における議論の例をあげてみることにする．

まず定義として，有限または無限の点列 $a_1, a_2, a_3, \cdots$ が単調減少であるというのは

$$a_1 \geq a_2 \geq a_3 \geq \cdots$$

が成立することとして，狭義に単調減少というのは

$$a_1 > a_2 > a_3 > \cdots$$

が成立することと定義する．

$$9, 9, 9, 7, 6, 6, \cdots$$

は単調減少で

$$100, 98, 76, 36, \cdots$$

は狭義に単調減少である.

いまつぎの簡単な定理とその証明をとりあげて，有限の立場から批判することにする.

定理 1 $a_1, a_2, a_3, \cdots$ を自然数の単調減少無限数列とする. このとき十分大きな自然数 n をとれば $a_n = a_{n+1} = a_{n+2} = \cdots$ となる.

(証明) $a_1, a_2, a_3, \cdots$ は単調減少であるからこのなかにでてくる可能性のある自然数は

$$0, 1, 2, \cdots, a_1$$

にかぎることは明らかであろう.

いま $a_1, a_2, \cdots$ のなかに 0 がでてくるかどうか，調べてみる. もしでてくるようならば，最初にでてくるところを a_n とすれば定理が証明された.

もし 0 が 1 回もでてこないとすれば，こんどは 1 について調べてみる. もし 1 がでてくるようならば，1 が最初にでてくるところを a_n とすれば定理は証明された.

もし 1 も 1 度もでてこなければこんどは 2 について同じことをくり返せばよい. このことを a_1 回だけくり返せば定理は証明される.

この証明は有限の立場の証明ではない. 有限の立場の証明でないところは，たとえば最初に 0 が $a_1, a_2, \cdots$ のなかにでてくるかどうか調べてみるところである. われわれ人間は有限のことしかできないから，調べていって有限回のうちにたまたま 0 にぶつかれば万歳であるが，そうでなければなんとも判定のしようがない.

もし自己に忠実で自分でほんとうに確認したものしか認めないで，確認しないものについて空想によって，または外からの超越的な権威によることを絶対にしないことにすれば，われわれはこのところを越えることができないのである.

懐疑的な人はただちに 2 つの疑いをもつであろう. その 1 つはここにのべた，証明が悪いのではないか？ ということであろう. しかしこれはあた

らない．どのように証明をかえてみても本質的な難点は同じである．少しばかり暇つぶしにやってみていただきたい．

第 2 の疑問は，そう神経質になるのならば，そのほかにもいろいろたくさんあるのではないか？　何もこのところにはかぎらないではないか？　しかもそんなに神経質になったら一切合財何もできなくなるではないか？　ということであろう．

これはもっとも至極の疑問である．このことについてのべるのは簡単ではない．しかしながら全体の筋道としてはつぎのようなことであるとご承知願いたい．

まず最初に素朴集合論における Russell のパラドックスやグラリフォルティのパラドックスによって集合概念に疑問がもたれたのであり，つぎにこれを契機として数学のなかのいろいろな概念についての反省が行なわれたのである．この結果どんなことに一番問題があるか？　どのようなことは厳密に行なえば合理化が行なわれるかが調べられた．そしてもっとも理想的な純粋な立場としてヒルベルトによって提出されたのがこの有限の立場なのである．そして有限の立場から批判して，上の証明で本質的な問題点はここに指摘したところなのである．

ここでわれわれの目的は有限の立場の「気分」を説明することであって，有限の立場について体系的に説明する暇はないが，もしこれ以上に興味のある方は小著

『数学基礎論』共立出版

を読んでいただきたい．

さてこのような純粋な立場をとる有限の立場で，いったい何か意味のあることが証明できるのであろうか？　これに徐々に答えるためにまずつぎの定理を証明しよう．

定理 2　自然数の狭義に単調減少な数列は必ず有限回で終ってしまう．

(証明)　有限の立場の証明はつぎのごとくである．

自然数の狭義に単調減少な数列

$$n_0, n_1, n_2, \cdots$$

があたえられたとする．これを n_0+1 回調べてみれば必ずその回に終ってしまうことは明らかである．

前の証明といまの証明との差は，前の証明は無限のものを調べることが前提となっており，こんどの証明は n_0+1 回という有限のものを調べることだけを要求していることである．

さてこの定理はあまりにも簡単であって，誰しもが，そんなに簡単なことならば何の不思議もないと思う可能性がある．だからもう少し複雑な定理を考えてみよう．はじめにまず定義をする．

定義　自然数の順序対 (m, n) についての辞書式順序 $<$ をつぎのように定義する．

$$(m_1, n_1) < (m_2, n_2)$$

とは $m_1 < m_2$ であるか，または $m_1 = m_2$ であって $n_1 < n_2$ であることと定義する．

もちろん断らないが順序対であるから

$$(m_1, n_1) = (m_2, n_2) \text{ とは } m_1 = m_2 \text{ で } n_1 = n_2$$

であることと定義する．

例を少しばかりあげれば，$(3,10)<(4,3)$ であり，$(3,8)<(3,9)$．またさらに $(2,4)<(3,6)$ というふうになる．

もちろん有限の立場でも，この大小の関係が自然数の順序対全体に線型順序をあたえることくらいは容易に証明することができる．

いま自然数の順序対の列

$$(m_1, n_1), (m_2, n_2), (m_3, n_3), \cdots$$

があたえられたとき，これが狭義に単調減少であるとは

$$(m_1, n_1) > (m_2, n_2) > (m_3, n_3) > \cdots$$

が成立することを意味する．例をあげれば

$$(5,3), (4,89), (4,36), (3,200), \cdots$$

は狭義に単調減少な列である．

さてわれわれの定理はつぎのものである．

定理 3　自然数の順序対の狭義に単調減少な列は有限回で終ってしまう．

（証明）　有限の立場での証明はつぎのようになる．

いま自然数の順序対の単調減少列

$$(m_1, n_1), (m_2, n_2), \cdots$$

があたえられたとする．このとき n_1+2 項目を調べてみよう．これを (m', n') とするとき明らかに $m' < m_1$ でなければならない．さてつぎにこの項から数えて $n'+2$ 番目の項を調べてみよう．この項を (m'', n'') とすれば $m'' < m'$ でなければならない．同じことを m_1+1 回続ければ，その間にこの列が終ることがわかるのである．

大切なことは有限回で実行可能なことを有限回実行することによって証明が，もっとハッキリいって事実を確認することが，完了するということである．

定理 3 は定理 2 に比べてだいぶ数学的になってきたが，この有限の立場ではいったいどの程度の数学が証明できるのであろうか？　これについて原則的に答えることはできないが，現在までの発展についてのべて，そのあとで小生の個人的な意見をのべることにしたい，

有限の立場の順序数

まずゲンツェン（Gentzen）の結果をのべるために，最初の ε_0 までの超限順序数についてのべることにする．順序数についてくわしくは集合論の本を見ていただくことにして，ここでは大ざっぱに説明することにすると，最初に自然数

$$0, 1, 2, \cdots$$

を考えて，すべての自然数が並んだ後に

$$\omega$$

という新しい数をもってきて，それから

$$\omega+1, \omega+2, \omega+3, \cdots$$

とさらに続けていくのである．すべての自然数について

$$\omega+n$$

を並べてしまって後に　　$\omega+\omega$

をもってきて，さらに

$$\omega+\omega+1, \omega+\omega+2, \omega+\omega+3, \cdots$$

と続けていく．すべての自然数 n について

$$\omega+\omega+n$$

を全部並べた後には　　$\omega+\omega+\omega$

をもってきて，その後へ　　$\omega+\omega+\omega+n$

と続けていく．簡単にするために，これを

$$\omega\cdot 3+n$$

と書くことにしよう．これをどこまでも続けると，一般に

$$\omega\cdot m+n$$

という形を全部書き並べたことになる．そのときその後に

$$\omega^2$$

を書き，それからいまと同じ手続きをすべてくり返して

$$\omega^2+\omega\cdot m+n$$

なる形のものを書いていく．この形が全部つくした後では

$$\omega^2+\omega^2$$

を書くのである．このようにしていくと

$$\omega^2\cdot l+\omega\cdot m+n.$$

その後に　　ω^3

を書いて，またさらに続けると一般に

$$\omega^k\cdot m_1+\omega^{k-1}\cdot m_2+\cdots+m_{k+1}$$

を全部つくすことができる．この後には

$$\omega^\omega$$

を書いて，またさらに続けていくのである．この操作を

$$\omega, \omega^{\omega}, \omega^{\omega^{\omega}} \varepsilon \cdots$$

と続けていってできるものを最初の ε-数までの順序数というのである．有限の立場での定義はつぎのようになる．（ここでは最初の ε-数までの順序数というかわりに，単に順序数という．）

1.　0 は順序数である．

2.　α と β とが順序数であるとき $\alpha+\beta$ は順序数である．

3.　α が順序数であるとき ω^{α} は順序数である．

4.　以上によってできたもののみが順序数である．

くわしい説明は前にあげた本を読んでいただくことにして，ここで順序数とは，0 と + と ω を組み合わせた図形のことを意味している．

もちろん実際には ω^0 のことを 1 と書くとか，1+1 を 2 と書くとか，ω^1 を単に ω と書くとか，いろいろの約束をしなければならないが，ここでは省略することにする．

さて，つぎにこの順序数について ＝ と ＜ とを定義しなければならない．たとえば $\alpha+0$ と α とはつねに等しいと考えるのである．また $\alpha_1+\cdots+\alpha_n$ を並べかえてできたもの $\beta_1+\cdots+\beta_n$ はもとの順序数と等しいと定義するのである．

＜ の定義はいささかやっかいである．だいたいにおいて

1.　$\alpha<\beta$ ならば $\omega^{\alpha}<\omega^{\beta}$.

2.　$\alpha_1+\cdots+\alpha_n<\beta_1+\cdots+\beta_m$ ならば $\alpha+\alpha_1+\cdots+\alpha_n<\alpha+\beta_1+\cdots+\beta_m$.

3.　$\alpha_1<\omega^{\beta}, \cdots, \alpha_n<\omega^{\beta}$ ならば $\alpha_1+\cdots+\alpha_n<\omega^{\beta}$.

というふうに定義するのである．

くわしいことは省略するが，2 つの順序数 α と β とがあたえられたとき，

$$\alpha<\beta, \quad \alpha=\beta, \quad \beta<\alpha$$

のいずれか 1 つだけが成立するのであるが，そのどれであるかを有限回できちんと判定する方法があたえられる．この順序数についてつぎの定理が成立する．

定理 4　順序数の狭義に単調減少な列

$$\alpha_0 > \alpha_1 > \alpha_2 > \cdots$$

は有限回で終ってしまう．

この定理の証明は超越的な集合論のなかでもそれほど簡単ではないが，ゲンツェンはそれを有限の立場で証明したのである．ゲンツェンは，さらにこの定理を用いて，自然数論の無矛盾性の証明を有限の立場で遂行したのである．

これはすばらしいことである．しかし現在までゲンツェンの証明に対して数学界は誤解で充満しているようである．たとえば，ある高名な数学者は‘ゲンツェンとは，数学的帰納法の無矛盾性の証明を超限帰納法を用いて証明した奴（guy）である’といっている．こういう発言はたいていの場合，身勝手な偏見に基づいて，ろくに物を考えないで感情的な発言をしているのだから，別にとりあげる必要はないが，じつは誤解の原因はわれわれ有限の立場側の方にも責任があるのである．もっとくわしくいえば，定理 4 の証明が有限の立場で遂行できるということが，ゲンツェンの証明においてはあまりキチンと説明されていないし，たとえば先にあげた小著の証明にしても，そのことがハッキリわかるように説明されていないのである．

これはもちろんあまりよいことではないが，じつはそれをキチンと書くということは言うはやすいが実行は大変なことなのである．私は最近証明論の本を書くことになって，そのへんをハッキリわかる程度に詳説したのであるが，じつに大変な仕事であった．だいたい専門家ならばこれでわかるであろうというふうに甘えてしまうということになりがちである．しかしながら定理 3 の証明の手法を精密にくり返しくり返し用いることによって定理 4 は証明されるのであって，上に引用した偏見にみちた誤解とは異なって，証明されないものを頭から用いたものではないし，またその有限の立場における純粋な証明は実行可能なのである．

ただいつでも，有限の立場における証明，ひいては無矛盾性の証明につい

ていえることであるが，その証明は超越的な集合論における証明より，かえって複雑でむずかしくなってしまう．これはきわめて純粋で弱い立場でむずかしいことを行なおうとするのであるから当然ではあるが，実際には多くの人々に敬遠される原因になってしまう．専門家にとっては残念なことだけれどもいたしかたのないことである．

さて，有限の立場においてゲンツェンの仕事を超えていくと，どこまでいけるのであろうか？　これについては筆者のつぎの結果がある．

筆者は有限の立場における ε_0- 数までの定義をさらに発展させて ordinal diagrams というものを定義して，その狭義単調減少列が有限回で終ってしまうことを証明し，それを用いて $\prod_1^1$-comprehension axioms の無矛盾性を証明したのである．ここに $\prod_1^1$-comprehension axioms というのは，ちょっと説明しにくいが，

$$\{x|A(x)\}$$

($A(x)$ をみたす x 全体の集合) というふうに新しい集合を定義する方法を一般に comprehension axioms というのであるが，上の公理はだいたいにおいて $A(x)$ のなかに‘すべての集合について’という論理記号が 1 回だけ入っているものと思ったらよい．自然数論は集合概念を本質的に含まないので，$\prod_1^1$-comprehension axioms の場合が本質的に集合概念を含む最初の場合といってよいであろう．

ところで，この ordinal diagrams というのは，集合論的に見ても厄介極まるものである．それを有限の立場で証明するというのは，もし詳細にすることを要求するならば，ほとんど不可能といってよいであろう．事実いままでに出版された，‘狭義単調減少列は有限回で終ってしまう’という ordinal diagrams についての定理の証明は有限の立場で証明できることがホノメカされているだけで，実際には inductive definition という集合論的原理が用いられているのである．このため筆者の無矛盾性の証明のあとに，Feferman は inductive definition を根本的な原理として採用することにより，小生の無矛盾性の結果がはるかに簡単に得られるということを証明して，彼自身は

これが筆者の結果の非常にエレガントな改良と信じているようである．しかしこれは筆者にとってはいささか本末転倒したことのように思われる．なぜならば，ordinal diagrams という特定のものについての inductive definition は有限の立場で遂行することのある糸口をあたえるのであるが，一般的に考えられた inductive definition というのはきわめて集合論的な性格で，これをもとにして無矛盾性の証明をすることはあまり意味がないと思えるからである．

しかしこのようなことを議論しても（実際に 1968 年に Feferman と公開の席上でちょっと，そのあとで個人的に長い間議論したが，満足のいく結論に至らなかった）あまり意味がないので，いま私はこんど出版する予定の証明論の本のなかで，どのように有限の立場のなかで遂行するかというoutline を書いているのである．残念なことにこの outline でさえ複雑で難解である．しかしながらだいたいの感じをいうならば，ordinal diagrams のような具体的な構造が有限の立場できちんとあたえられたならば，その構造をいくらでも細かく調べていくことは有限の立場でも可能であり，その構造の細かい性質を調べたあとでは，いくらでもうまい証明の方法を見つけることができるのである．実際にゲンツェンの場合の証明にも，よく観察してみれば，最初の ε- 数までの順序数の内部構造を上手に用いることによって定理の証明が有限の立場で遂行されているのである．

さて，内容をのべることなしに机上の説明をだいぶしてしまったが，有限の立場でいったいどれだけ数学が構成できるのであろうか？　私の意見は，どこまででもできるというものである．もちろん有限の立場で証明できないものはいくらでもあるのであるが，私のいうどこまでもというのは，集合論の無矛盾性も，もっと強い理論の無矛盾性をいえるようなものまでも有限の立場で作っていくことができるだろうということである．これは非常に楽観論であるが，私自身のなかにこれとは多少異なった意味で極端な悲観論がある．それはいままでの経過から推して，数学的内容が加速度的にむずかしくなっていき，またそれにしたがって，その定理が実際に有限の立場で遂行さ

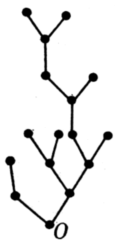
れるということを説明するのが事実上不可能になっていきはしないか，ということである．

このように有限の立場は，実際には大変な難関を未来にもっているものであるが，数学の基礎についての立場としてはやはり一番純粋で重要なものであると私は思うのである．

直観主義について

有限の立場についてのべたついでに，直観主義について少しばかりのべることにする．直観主義というのは大ざっぱにいえば，有限の立場と超越的な集合論的立場の中間にあるようなものである．それはたとえば点列というようなものについて，有限の立場では考えられないような抽象的な発言をするのであるが，といって集合論的な考え方も極端に嫌うのである．一般論はこれくらいにして，具体的な例について考えることにしよう．いまつぎのケーニッヒの定理の集合論的な証明を考えよう．

定理 5　いま下図のように 1 つの点 O から出発して毎回高々 2 つに枝分れする図形を考えよう．



いまこの図形において O から上へ上へとある枝を通って登っていったとする．そのときどの枝を通っていっても必ず有限回で終ってしまうものとするとき，じつはこの図形は有限個の点と枝でできている．

（証明）　もしそうでないとする．O から出発して考えることにする．O は高々 2 点 O_1, O_2 とに枝分かれするわけである．（もし 1 つも上になければ，図形は O だけだからそれでよい．また O から枝はたった 1 つだけで O_1 だけにつながっているとすれば，O_1 をつぎに O' として考えればよい．）ゆえにもし O の上に無限の点があるとすれば，O_1 と O_2 のどちらかの上に無限の点がなければならない．いま O_1, O_2 のうちでその上に無限の点がある方の 1 つを O' とする．さて O' は高々 2 つの点に枝分かれしているわけである．このうちの少なくとも 1 つはその上に無限の点がなければならない．そのようなものをとってきて O'' とする．このように $O', O'', O''',$ … ととってくると，これはいつまでたってもつきない．ゆえに定理の仮定に矛盾する．

この証明は，もちろん有限の立場における証明ではない．なぜならば，O の上に無限の点があるとして，O_1 か O_2 のどちらかに無限の点があるとして，そのような点の 1 つをとってくるからである．有限の立場での疑問はどうして，どんな方法で O_1 と O_2 とのどちらを選べばよいかがわかるのか？ということである．すなわち有限の立場では O' を見つける方法がありえないのである．

直観主義では，有限の立場と同じく無限にあるものを全部調べるということを拒否するのであるが，この定理自身は認めるのである．その理由は私にはどうも判然としない．1 つだけわかるのは直観主義では集合論とは異なった，しかし非常に強い数学が作りたいからである．私などにとっては直観主義は必要に応じて集合論からカンニングをするのではないか？と思うのだが，これはどうも人の悪い見方かもしれない．もっとも上の定理は直観主義のなかでは一番理解し易い場合であって，実際には自由選別という，曰くいい難きものについて直観主義者は神秘的な直観をもっているのであるが，残念なことに直観主義者もその個人個人によって直観が異なるらしく，以前にきいたところでは 40 くらいの異なった公理があって，どれがほんとうかよ

くわからないとのことであった．

しかしながら直観主義に有限の立場のような純粋性を要求しなければ，直観主義者のやっていることの意味はわかり易い．それは集合論において新しい公理を要求しているように，とくに強い無限の公理を求めているように，直観主義では無限のものを固定した絶対と考えることは避けながらも，abstract notion には積極的に考え，game をいどみ，新世界の創造に努力しているものといってよいであろう．

筆者は有限の立場を finite mind の世界，集合論を infinite mind の世界，直観主義を abstract mind の世界と分類するのであるが，それぞれに意味のある面白い世界だと思っている．ただ abstract mind がいまのところ一番ハッキリしない不安定な mind のように思うのである．したがって私の直観主義に対するおもな批判はハッキリしないとかアイマイであるとかいうことになる．たとえば（ちょっと専門用語を用いさせてもらうが）いまここに primitive recursive predicate $\prec$ があったとして，集合論によって $\prec$ が整列であることが証明されたとする．そのとき，ある直観主義者が彼の直観にしたがって $\prec$ が整列であることが明らかである，といったときに，このことを正しいと思ったり誤っていると思ったりする判断の基準はどこにあるのだろうか？　かなりの数学者ならば，集合論的な証明に精通してくればだんだん直観的に正しいと思えてくるのではないだろうか．そしてまたこのことがナンセンスだとすると，上のケーニッヒの定理が直観主義的に正しいということは，定理が易しくてわかり易いというほかに，ほんとうに理由があることなのであろうか？

有限の立場や，集合論の程度に透明な直観主義ができあがることを期待してやまない．

ウント大きな自然数

大きな数のコンテスト

多勢の人にウント大きな自然数をいわせるコンテストをしたらどんなことになるだろうか？　もちろん一番大きな自然数をいった人が勝ちということにするのである．

よく落語などではつぎのような状況にお目にかかる．A, B, C の 3 人の人にウント大きな自然数をいわせる競争をさせる．Aがしばらく考えてなかなかうまいことをいう．つぎに B がもうしばらく考えて数段うまいことをやってのけてドウダという顔をする．すると C がアッサリと B のいった数にプラス 1 というようなことをいう．これは落語としては面白い．A, B の苦労と巧みさに比べて，C が労せずして勝つというコントラストが落ちなのである．しかし考えてみると，これは単に後手必勝法，それも至極簡単な後手必勝法が存在するということにほかならない．このような簡単な後手必勝法が存在するゲームでは先にいい出す方がバカである．いまもしこの間の事情を知っている 2 人にこのゲームをさせたらどうなるだろうか？　キット 2 人ともダマッテ相手のいい出すのを待っているにちがいない．したがって最初のゲームはダンマリのゲームか忍耐心のゲームか，それでなければはじめから引き分けと結果がわかっているちがったゲームに移行してしまう．

しかしこれは 2 人一緒にして競争させるから困るのであって，じつはゲ

ームは 2 人を別々にして独立に答を書かせるべきであろう．そうするとどうなるだろうか？　A,B と 2 人いるときに，フタをあけてみたら，A は ‘B の答プラス 3’　B は ‘A の答プラス 5’ と書いてあったとしたら，どちらが勝ちとすべきだろうか？　そういう場合は望ましくないので，互いに相手の答には関係しない答を書くということにしなければならない．こう制限してもまだ困ることがある．よけい時間をかければ，いくらでも大きい自然数が作れるのでドウシテモ勝ちたいと思う人はいつまででもネバルであろう．これもあまり面白いことではないのでわれわれは時間を 10 秒というふうに決めて‘用意’‘始め’とゲームを開始しなければならない．もっともこれでもまだ苦情があるにきまっている．鉛筆を早く動かす技術がある方が有利にきまっている．しかしこれもゲームのうちと思って辛抱していただくことにする．

さて皆さん，皆さんだったら何を書きますか？

さてここで最初の落語の A,B,C 3 人の人にふたたびご登場を願うことにしよう．皮肉なことに，このゲームでは事情はふたたび逆転してしまう．A と B のアイディアはここではそれなりに有効であるが，C のアイディアはここではまったく有用ではない．

$$1+1+1+\cdots$$

と続けていったのでは 10 秒に書ける数は知れている．

10 の巾乗

さて皆さん．皆さんは何を書きましたか？　たいていの人が何の予備準備もなしに不意にこういうゲームに参加させられたら答はつぎのようになるのではないだろうか．

$$10^{10^{10^{10^{10^{10}}}}}$$

ここでじつをいうと，巾（ベキ）にカッコをどうつけるかが大切である．

$$10^{\left(10^{\left(10^{10}\right)}\right)} \quad と \quad \left(\left(10^{10}\right)^{10}\right)^{10}$$

とでは大変な差である．

もっと簡単なところでやってみれば

$$10^{\left(10^{10}\right)} \quad は \quad 10^{10000000000}$$

であるが

$$\left(10^{10}\right)^{10} \quad は \quad 10^{100}$$

にすぎない．これは巾を 2 回くり返したにすぎないが，上の 3 回のときのカッコのつけ具合による差はいまの場合とは比較にならない．これは 3 回が 4 回になり 5 回になるにしたがって，ますますはなはだしくなるのである．

さて，ここでちょっと考えてみよう．われわれは急に短い間にウント大きな自然数を書けといわれると，とかく 10 の巾の巾の巾…というふうに考えがちであるが，その理由は何であろうか？　10 と書くのはあまり意味がない．トッサに書ける数のなかではこれが一番簡単で手軽である．たとえば 25 などと比べてみればよくわかる．もっとヒネッテ考えても 9^9 などからみてはるかに簡単である．ちょっと考えてみても

$$100^{100} \quad と \quad 10^{10^{10}}$$

の手間がほとんど同じだと思えば，10 という数がいまのアラビア数字による 10 進法のなかでは抜群に書き易く，こういう場合には便利な数である．意地の悪い人は，11 の方がもっと書き易くて 10 より大きいではないか？といわれるだろうが，それはまったくもっともであるが，ここではあまり本

論に関係がないのでご容赦願いたい．（しいていえば私が 10 の方を 11 より選ぶのは，10 の方が心理的にこころよいということらしい．10 と 11 とでは大きさはほとんどかわらないのであるから，たくさん書くときには心理的にこころよい方が能率的であろう．）

function は functional

さて10の使用について自分自身をなっとくさせるのはこれくらいにして，こんどは巾の方を考えてみることにしよう．どうして，ドンドン大きな自然数をほしいと思うとっさの場合に，われわれは巾を用いようとするのだろうか？

この説明には少しばかり手間がかかるように思われる．まず自然数は0から出発して，1 を加えていけばどれだけでも大きい自然数を得ることができる．したがって時間の制限がなければ，このノンビリした方法を用いることに原則的な反対はない．しかしわれわれはいま大きな自然数をうんと能率よく得たいということなので，この考えは都合が悪いというわけである．もっと機能的な方法を探さねばならない．機能的といったときに，いままでの伝統的な数学ですぐ頭に浮かぶのは関数である．（これは多くの場合意識されることが少なく，たいていは本能的に無意識的に考えられる．たとえば上の例のような場合でもこのような考えは無意識にされる．）さて原則的に可能ではあるが能率の悪い方法，「1 を加える」を関数の形で書けば

$$f(x)=x+1$$

となる．この関数は

1.1)　$x<y \rightarrow f(x)<f(y)$

1.2)　$x<f(x)$

なる 2 つの性質をみたしている．

ちょっとした注意をつけ加えるならば，1.1) のもとでは 1.2) は

1.2′)　$0<f(0)$

でおきかえてもよい．

いまこの 2 つの条件をみたしている任意の関数 $f(x)$ をとってくるとき，勝手な数 a，たとえば 1 とか 10 とか，から出発して

$$f(a), f(f(a)), f(f(f(a))), \cdots$$

というふうに f をくり返していけば，原則的にはいくらでも大きな自然数が得られるわけである．問題はいかにして能率よく急激に大きくなる関数 f を見つけるか？ということである．

ここで前にのべた関数が機能的（英語でいえば function が functional）であるということを説明すると，単独の大きな自然数を個々に考えるよりは，能率のよい関数 $f(x)$ を考えて，この f をくり返すことによって大きい自然数を得る方が全体的な考察がし易く，はるかに機能的である．

いまここで $f(x)$ がわれわれの目的で能率よいということを直観的な意味で使ったが，これはもちろんどんどん大きくなる能率がよいということを意味するわけであるが，数学的にはどうのべたらよいであろうか？

いま 2 つの関数 $f(x), g(x)$ があたえられたときに，‘$g(x)$ の方が $f(x)$ より能率よく大きくなる’ということを

$$f(x) \prec g(x)$$

と書いて

$$\exists k \forall x (k < x \rightarrow f(x) < g(x))$$

で定義する．ここで論理記号の説明をするいとまはないが，上の式を読んでみれば，頭から順に

ある自然数 k が存在して，すべての自然数 x について，$k < x$ ならば $f(x) < g(x)$ が成立する．

と読むのである．

この関数についての関係 $\prec$ は あとで「ゲーデルの新しい公理について」にもでてくるが，ここではあまり高級な性質は用いない．ただ 1 つだけ説明すれば，この定義では関数の最初の部分はあまり問題にしないようになっている．これはじつは妥当なことである．たとえばわれわれは乗法は加法より大きくなるという漠然たる気持ちをもっているが，この定義にあてはめる

ならば

$$f(x)=x+x=2\cdot x$$

$$g(x)=x\cdot x=x^2$$

とすればまさしく $f\prec g$ という関係によってわれわれの感じている気持ちを表わすことができるのである．もちろん関数のはじめの部分だけを考えれば

$$g(1)=1<2=f(1)$$

となって，逆に加法の方が乗法の方よりも大きいことがありうるのである．

さて能率よく大きくなるということについても，数学的定義ができたが，いよいよどうやって能率よく大きくなる関数を得るか？ という問題のキイポイントにふれていくわけである．

定理 1 $f_1(x), f_2(x)$ が上の 1.1)，1.2) の条件をみたす関数であるとき，

$$g(x)=f_1(f_2(x))$$

とおけば，$g(x)$ も 1.1)，1.2) の条件をみたし，さらに

$$f_1\prec g \ \wedge\ f_2\prec g$$

である．ここに $A\wedge B$ は‘A であってかつ B である’と読む．

証明はほとんど明らかなので演習問題として残したい．

この定理はいま 1.1),1.2) をみたす関数 $f(x)$ があたえられたときには，$f(f(x)), f(f(f(x))), \cdots$ と $f(x)$ を何度もくり返したものを作ればそれはますます能率のよい関数を作ることを意味する．

いま $f(x)$ を n 回くり返してできたものを $f^n(x)$ とする．すなわち

$$f^n(x)=\underbrace{f(f(\cdots f}_{n\text{回}}(x)\cdots))$$

と定義することにすれば，

定理 2 $f(x)$ が 1.1),1.2) の条件をみたす関数とするとき，

$$g(x)=f^x(x)$$

と定義すれば，いかなる n に対しても

$$f^n\prec g.$$

（証明）　$x>n$ に対しては

$$f^n(x)<f(f^n(x))=f^{n+1}(x)<f^{n+2}(x)<\cdots<f^x(x)=g(x).$$

この定理は $g(x,y)=f^y(x)$ という 2 変数の関数を考えれば，$f,f^2,f^3,\cdots$ 全部より能率のよい関数が $g(x,x)$ を考えることによってただちに得られることを意味している．じつをいえば個々の大きい自然数を考えるよりは，能率よく大きくなる関数を考える方が機能的であるのと同じ理由で，能率よく大きくなる 2 変数の関数を考える方が個々の能率よく大きくなる関数を考えるよりはるかに機能的なのである．

しかも 1 変数の能率よく大きくなる関数を作る仕事と 2 変数の能率よく大きくなる関数を作る仕事とは，じつは同じ仕事とも考えられるのである．

いま 2 変数の関数 $g(x,y)$ があたえられて

2.1)　$x_1<x_2 \rightarrow g(x_1,y)<g(x_2,y)$

2.2)　$y_1<y_2 \rightarrow g(x,y_1)<g(x,y_2)$

2.3)　$0<g(0,0)$

の 3 条件をみたしているものとする．このとき

$$f(x)=g(x,x)$$

と定義すれば，$f(x)$ は 1.1),1.2) の 2 条件をみたし，そのうえに

$$g(x,y)<f(x+y)$$

がつねに成立するから，2.1),2.2),2.3) をみたす能率のよい関数から 1.1), 1.2) をみたす能率のよい関数を作ることができ，また逆に 1.1),1.2) をみたす能率のよい関数 $f(x)$ があたえられたときには

$$g(x,y)=f(x+y)$$

によって逆に g を定義すれば，g も f と同程度に能率のよい関数と考えられる．したがって 1 変数，2 変数ということは本質的ではなく，同じ問題が形をかえて表われているだけだと考えることができる．

巾乗の理由

さてだいぶ一般論に飛んでしまった．われわれはふたたび 10 の巾乗をく

り返すことについて説明しなければならない．

自然数の生成原理として用いられる一番基本的な 1.1), 1.2) をみたす関数

$$f_0(x)=x+1$$

から出発して考えよう．これから定理 1, 2 を用いて能率のよい関数を作ろうとすると，$g_1(x,y)=f_0{}^y(x)$ を作ることになる．これはいかなる関数であろうか？　明らかにわかるように，これは $x+y$ である．すなわちわれわれの一般論にしたがって能率のよい関数を作ると加法が自然に表われてくるのである．

さて，さらに $x+y$ からわれわれの一般論にしたがって能率のよい関数を作るためには，じつは $x+1$ という 1 変数の関数から $x+y$ という 2 変数の関数を作ったように，じつはこんどは 3 変数の関数を作るのが機能的な方法である．しかし変数がだんだんと増えてくるとだんだんとり扱いがやっかいになって面倒になってくる．実質は同じことであるから，ここではちょっとハショらしてもらって，

$$g_1(x,y)=x+y$$

として

$$h_2(x,y)=\underbrace{g_1(g_1(\cdots g_1(g_1}_{y\text{回}}(0,x),x)\cdots,x),x)$$

と定義すれば，前の定理 1 および定理 2 によって，$h_2(x,y)$ は $x+y$ よりはるかに能率のよい関数といってもよいであろう．容易にわかるように，これは

$$x\cdot y$$

なる乗法の関数を意味している．したがってこれは乗法が加法よりはるかに能率のよい関数であることを意味している．

同様の方法を継続していくとどうなるであろうか？

つぎにできる関数は

$$k_3(x,y)=\underbrace{h_2(h_2(\cdots h_2(h_2}_{y\text{回}}(1,x),x),\cdots,x),x)$$

すなわち

$$x^y$$

となって巾乗がでてくるのである．すなわちわれわれがトッサに思いつく能率よく大きくなる関数は，$x+1$ から出発して一般論にしたがって能率のよい関数を作るしくみにしたがって第 3 番目に得られる関数巾乗を何回もくり返してできる関数になっているわけである．

これはある意味でわれわれが 10 の巾乗をくり返すことの正当化になっている．それと同時にこの方法がいかに中途半端なものかも教えてくれる．たとえばわれわれの一般論にしたがってさらに第 4 番目に得られる能率のよい関数 $l_4(x,y)$ を作れば

$$l_4(x,y)=x^{\left(\cdots\left(x^{\left(x^{x}\right)}\right)\right)}\Big\}y\text{回}$$

がでてくるのである．

実際にわれわれが巾乗のくり返しを用いるのは，加法，乗法，巾乗までが実際によく用いられ，それ以上は普通数学ではとり扱われる機会があまりないので，実際によく知られているもののなかで best possible なものを選んだことになっている．

新しい問題の提起

さて大きな数を書くコンテストという実際の問題から具体的な 10 の巾乗をくり返して書くという方法についての考察にだいぶ紙数を費してしまった．ここで問題をより抽象的に考えることにすると，つぎに考えることはいったいどんなことであろうか？

最初の問題は，いま定理 1 と定理 2 の方法でいくらでも能率のよい関数が作れるか？という問題である．もっと数学的な表現をすれば $f_0(x)=x+1$ なる関数から出発して，代入と関数結合を y 回くり返してできる新しい y の関数にこのような方法を何度かくり返すことによっていくらで

も能率のよい関数ができるか？　という問題である．以下において問題の把握はこの程度でよいが，本書の「初等初等整数論」の概念を用いてつぎの正確な formulation を書いておくことにする．

primitive recursive function（以下 p.r.f. と略記）によっていくらでも能率よく大きくなる関数が作れるか？

ヒルベルトは連続体問題に関して この疑問と密接に関連したことを 1926年に提起した．

しかし，この問題の答は No！である．しかもその解答は本書の「ゲーデルの新しい公理について」のなかにあると思ってよい．すなわちもう少しくわしくいえば，p.r.f. の全体は高々可付番である．高々可付番の関数があたえられたときに，そのどれよりも $\prec$ の意味で大きい関数を作る方法がそのなかにあたえられているからである．しかしながらこのような具体的な問題にはできればもっと具体的な解答がほしい．具体的なもっとハッキリ定義される関数を実際に構成して，できればその面白い性質をいろいろと調べてみたい．Ackermann はこのような関数を提出して，1928 年に，ヒルベルトの提起した問題を解決したのである．以下に Ackermann の関数についてのべることにする．

Ackermann の関数

Ackermann の関数はつぎの 3 式によって定義される．

3.1)　$$f(0, y)=y+1$$

3.2)　$$f(x+1, 0)=f(x, 1)$$

3.3)　$$f(x+1, y+1)=f(x, f(x+1, y))$$

このような $f(x, y)$ がただ1通りに定義されることは x と y とについての2重帰納法から明らかであろう．以下にこの Ackermann の関数 $f(x, y)$ の性質を順々にのべていくことにする．

定理 3

1)　$$y<f(x, y)$$

2) $$f(x, y) < f(x, y+1)$$

3) $$f(x, y+1) \leqslant f(x+1, y)$$

4) $$f(x, y) < f(x+1, y)$$

5) $$f(1, y) = y+2$$

6) $$f(2, y) = 2y+3$$

7) $$f(x_1, y) + f(x_2, y) < f(x^*, y)$$

ここに $x^* = \max(x_1, x_2) + 4$.

(証明)　1) の式がすべての y について成立することを，x についての数学的帰納法で証明する．すなわち

$$\forall y\,(y < f(x, y))$$

が帰納法の仮定である．この仮定のうえで $y < f(x+1, y)$ を y についての帰納法で証明する．

$$f(x+1, 0) = f(x, 1) > 1$$

$$f(x+1, y+1) = f(x, f(x+1, y)) > f(x+1, y) > y$$

の 2 式から明らかである．

2)　x についての数学的帰納法で証明する．

$$x = 0$$

のときは明らか．

$$x+1$$

のときは 1) を用いて

$$f(x+1, y) < f(x, f(x+1, y)) = f(x+1, y+1).$$

3)　y についての数学的帰納法．

$$y = 0$$

のときは 3.2) より明らか．

$$y+1$$

のときは 1) により　　$y+1 < f(x, y+1)$

ゆえに　　$y+2 \leqslant f(x, y+1) \leqslant f(x+1, y)$　　(帰納法の仮定より)

ゆえに　　$f(x, y+2) < f(x, f(x+1, y)) = f(x+1, y+1)$

ここに最初の不等号は 2) を用いた.

4) $$f(x,y)<f(x,y+1)\leqslant f(x+1,y). \qquad (\ 2),3)\ より)$$

5) y についての数学的帰納法.

$$f(1,0)=f(0,1)=2$$

$$f(1,y+1)=f(0,f(1,y))=(y+2)+1=(y+1)+2.$$

6) y についての数学的帰納法.

$$f(2,0)=f(1,1)=1+2=3=2\cdot 0+3$$

$$\begin{aligned} f(2,y+1)&=f(1,f(2,y)) \\ &=f(2,y)+2 \\ &=2y+3+2 \\ &=2(y+1)+3. \end{aligned}$$

7)
$$\begin{aligned} &f(x_1,y)+f(x_2,y) \\ &\leqslant f(\max(x_1,x_2),y)+f(\max(x_1,x_2),y) \\ &<2f(\max(x_1,x_2),y)+3 \\ &=f(2,f(\max(x_1,x_2),y)) \\ &<f(\max(x_1,x_2)+2,f(\max(x_1,x_2)+3,y)) \\ &=f(\max(x_1,x_2)+3,y+1) \\ &\leqslant f(x^*,y). \end{aligned}$$

つぎに Ackermann の関数はすべての p.r.f. より大きいということがいえる．これはつぎの定理の形で証明される．

定理 4　$g(x_1,\cdots,x_n)$ を任意の p.r.f. として $f(x,y)$ を Ackermann の関数とする．このとき十分大きい c が存在して，すべての $x_1,\cdots,x_n$ に対して

$$g(x_1,\cdots,x_n)<f(c,x_1+\cdots+x_n)$$

が成立する．

(証明)　$g(x_1,\cdots,x_n)$ の構成の仕方にしたがって証明する．

すなわち $g(x_1,\cdots,x_n)$ を構成するために用いられた p.r.f. については,

もうすでに定理が証明されているものとする．

1) $$g \text{ が } x+1$$

のときは $$c=1$$

ととればよい．すなわち $$g(x)<f(1,x)$$

2) $$g(x_1,\cdots,x_n) \text{ が } x_i$$

のとき $$c=0$$

とすればよい．

$$x_i<f(0,x_1+\cdots+x_n)$$

3) $$g(x_1,\cdots,x_n)=h(g_1(x_1,\cdots,x_n),\cdots,g_r(x_1,\cdots,x_n))$$

であるとき，このとき

$$h(y_1,\cdots,y_r)<f(c,y_1+\cdots+y_r)$$

$$g_1(x_1,\cdots,x_n)<f(c_1,x_1+\cdots+x_n)$$

$$\vdots$$

$$g_r(x_1,\cdots,x_n)<f(c_r,x_1+\cdots+x_n)$$

なる $c,c_1,\cdots,c_r$ がすでに見つかっているとする．

$$\begin{aligned}g(x_1,\cdots,x_n)&=h(g_1(x_1,\cdots,x_n),\cdots,g_r(x_1,\cdots,x_n))\\&<f(c,g_1(x_1,\cdots,x_n)+\cdots+g_r(x_1,\cdots,x_n))\\&<f(c,f(c_1,x_1+\cdots+x_n)+\cdots+f(c_r,x_1+\cdots+x_n))\end{aligned}$$

いま $$\tilde{c}_1=\max(c_1,c_2)+4$$

$$\tilde{c}_2=\max(\tilde{c}_1,c_3)+4$$

$$\vdots$$

$$\tilde{c}_{r-1}=\max(\tilde{c}_{r-2},c_r)+4$$

とおけば $$\begin{aligned}&f(c_1,x_1+\cdots+x_n)+\cdots+f(c_r,x_1+\cdots+x_n)\\&\quad<f(\tilde{c}_{r-1},x_1+\cdots+x_n)\end{aligned}$$

ゆえに $$\begin{aligned}g(x_1,\cdots,x_n)&<f(c,f(\tilde{c}_{r-1},x_1+\cdots+x_n))\\&<f(c+\tilde{c}_{r-1},f(c+\tilde{c}_{r-1}+1,x_1+\cdots+x_n))\\&=f(c+\tilde{c}_{r-1}+1,x_1+\cdots+x_n+1)\\&\leqq f(c+\tilde{c}_{r-1}+2,x_1+\cdots+x_n)\end{aligned}$$

ゆえに $c+\tilde{c}_{r-1}+2$ が求めるものである．

4)
$$g(x_1, \cdots, x_n, 0)=h_1(x_1, \cdots, x_n)$$
$$g(x_1, \cdots, x_n, y+1)=h_2(x_1, \cdots, x_n, y, g(x_1, \cdots, x_n, y))$$

によって g が定義されているとき，ここに

$$h_1(x_1, \cdots, x_n)<f(c_1, x_1+\cdots+x_n)$$
$$h_2(x_1, \cdots, x_n, y, z)<f(c_2, x_1+\cdots+x_n+y+z)$$

なる c_1, c_2 はすでに見つかっているものとする．この c_1, c_2 から

$$h_1(x_1, \cdots, x_n)+x_1+\cdots+x_n<f(c_1^*, x_1+\cdots+x_n)$$
$$h_2(x_1, \cdots, x_n, y, z)+x_1+\cdots+x_n+y+z<f(c_2^*, x_1+\cdots+x_n+y+z)$$

なる c_1^*, c_2^* は容易に定理 3 の 7) および本定理の 2) により容易に見つかる．いま

$$c=\max(c_1^*, c_2^*)+1$$

が求めるものであることを

$$g(x_1, \cdots, x_n, y)+x_1+\cdots+x_n+y<f(c, x_1+\cdots+x_n+y)$$

を y についての帰納法で証明することによって証明する．

$$y=0$$

のとき，
$$g(x_1, \cdots, x_n, 0)+x_1+\cdots+x_n<f(c_1^*, x_1+\cdots+x_n)$$

$$y+1$$

のとき，
$$\begin{aligned}&g(x_1, \cdots, x_n, y+1)+x_1+\cdots+x_n+y+1\\ &=h_2(x_1, \cdots, x_n, y, g(x_1, \cdots, x_n, y))+x_1+\cdots+x_n+y+1\\ &<f(c_2^*, x_1+\cdots+x_n+y+g(x_1, \cdots, x_n, y))+1\\ &<f(c_2^*, f(c, x_1+\cdots+x_n+y))+1\\ &\leqslant f(c-1, f(c, x_1+\cdots+x_n+y))+1\\ &=f(c, x_1+\cdots+x_n+y+1)+1\end{aligned}$$

このなかで $<$ が 2 回表われているから

$$g(x_1, \cdots, x_n, y+1)+x_1+\cdots+x_n+y+1<f(c, x_1+\cdots+x_n+y+1)$$

となって定理が証明された．

定理 5 Ackermann の関数 $f(x, y)$ は p.r.f. でない．

(証明)　　$f(x,y)$ が p.r.f.

であるとすると　　$g(x)=f(x,x)$ も p.r.f.

であり前定理より　　$g(x)<f(c,x)$

なる c が存在する．これは

$$g(c)=f(c,c)<f(c,c)$$

となって　　矛盾する．

むすびに

すべての p.r.f. より能率よく大きくなる関数は上に見るように Ackermann の関数によりみごとに解決された．しかもこの Ackermann の関数は内容的には

$$\xi_0(b,a)=a+b$$

$$\xi_1(b,a)=a\cdot b$$

$$\xi_2(b,a)=a^b$$

$$\xi_3(b,a)=a^{a^{\cdots^{a}}}\Big\}b\text{ 回}$$

一般には

$$\xi_{n+1}(0,a)=a$$

$$\xi_{n+1}(b+1,a)=\xi_n(\xi_{n+1}(b,a),a)$$

とおいて

$$\xi(n,b,a)=\xi_n(b,a)$$

によって自然に定義された，加法，乗法，巾乗といった考えを延長してできた関数にちょっとした変形を加えたものであるから，その意味は明瞭なものといってよいだろう．

このような仕事を先へ進めていくと，算術の言葉（+, ·, = と論理記号）で表わされるすべての関数より能率よく大きくなる関数，集合論の言葉で表わされるすべての関数より能率よく大きくなる関数をなるべくみごとに定義するというような問題がでてくる．このような数学基礎論に密接な整数論的

関数はいまのところ伝統的な整数論的関数とあまり関係がないようである．というよりは現在の時点では，数学基礎論的整数論と伝統的整数論との間には深い gap があるように思われる．この gap を埋めていくことは数学基礎論にたずさわる人にとっての 大切な 1 つの課題であるように思われる．上にのべたような問題の行方には，たとえば，フェルマーの問題や，ゴールドバッハの問題がペアノの自然数論のなかでは証明できないというような興味津々たる問題がひかえているのである．このような進路をとることがまた逆に伝統的な整数論に対してもよい刺激であることは十分考えられるところである．この最後にのべたところは，そのうちにユックリとおりをみて議論してみたいと思っている．

ニセモノ自然数

自然数の公理

ここでやろうとすることは，自然数全体とソックリな性質をもっているけどじつは自然数全体とは全然異なるものを代数的な手法で作りだそうということである．代数学の初等的な知識は仮定するが高級な知識は仮定しない．

まず最初にソックリということの意味について，またそれについての論理学からの一般論について説明するが，われわれの本当の目的はよく知られている代数的な構成のなかから自然数全体にソックリなものを作ることにあって，抽象的な論理学での構成に興味があるわけではない．論理学の方はすぐ姿を消してしまう前座だと思って気長におつきあいを願いたい．

自然数とここでいうのは 0, 1, 2, … のことである．といってもただ自然数といって 0, 1, … と並べただけではあまり意味がない．実際にはその性質をこめて考えているのである．自然数の性質といってもたくさんあるが，ここではきわめて初等的なものだけ考えることにする．もっとくわしくいうと，

特別な自然数として

$$0$$

自然数の上の predicate（述語）として

$$=$$

自然数の上の関数として

$$',\ \delta,\ +,\ \dot{-},\ \cdot$$

と 5 つの関数だけを用いることにする．ここにちょっとだけ説明を加えると，$+$ と $\cdot$ は普通の加法と乗法である．a' は $a+1$ のことであり，$a\dot{-}b$ は a が b より小さいときは 0，そうでないときは普通の減法を表わすものとする．$\delta(a)$ は $a\dot{-}1$ のことである．もう 1 つだけ注意をすると自然数は全部 0 と $'$ だけで表わされる．$1=0', 2=0'', \cdots$ というふうにである．しかし以下には普通の通り，$1, 2, 3, \cdots$ を用いる．しかしこれはつねに省略記号であると思ってほしい．たとえば 5 と書けば本当は $0'''''$ のことだと思っていただきたいのである．

さて，これらの基本的な記号についての自然数のもつ性質は何であろうか？　普通はそのなかで最も基本的なものを公理として採用して，あとは論理だけの推論で公理から導きだすのである．公理系のとり方もいろいろとあるがいずれも大同小異で，通常いずれもペアノの公理と呼ばれている．ここでは $a, b, c, \cdots$ は任意の自然数を表わす変数として，その公理を書いてみる．

1)　$=$ について

1.1)
$$a=a$$

1.2)
$$a=b \rightarrow b=a$$

1.3)
$$a=b \wedge b=c \rightarrow a=c$$

ここで $\wedge$ は‘そして’と読む．

1.4)
$$a=b \wedge P(a) \rightarrow P(b)$$

ここに $P(a)$ は a についての任意の性質であるとする．この $=$ についての公理群は，論理についての性質であるとして，あらためて書かないことが多い．

2)　$0,\ ',\ \delta,\ +,\ \dot{-},\ \cdot$ について

2.1)
$$\neg a'=0$$

$\neg$ は‘でない’と読む．$\neg a=b$ はしばしば $a\neq b$ と略記される．

2.2)
$$\delta(0)=0$$

2.3)
$$\delta(a')=a$$

2.4) $$a+0=a$$

2.5) $$a+b'=(a+b)'$$

2.6) $$a\cdot 0=0$$

2.7) $$a\cdot b'=a\cdot b+a$$

2.8) $$a \dot{-} 0=a$$

2.9) $$a \dot{-} b'=\delta(a \dot{-} b)$$

このほかに数学的帰納法の原理をつぎの推論の形で入れることにする.

3)　数学的帰納法

$$\frac{P(0) \qquad P(a)\rightarrow P(a')}{P(a)}$$

この推論方法の意味は，$$P(0)$$

が成立し，さらに任意の自然数 a について，

$$P(a) \rightarrow P(a')$$

が成立するならば，任意の自然数 a について

$$P(a)$$

が成立する，ということであり，ここに $P(a)$ は a についての性質である.

ソックリなニセモノということ

さて多少の準備ができたから，ここで，ソックリのニセモノということについて説明しよう．ソックリということは自然数がみたす性質を全部またはカナリみたすということと，ここでは考えることにする．ニセモノというのは，しかしながら自然数とは異なるということである.

最初に注意すべきことは，上にのべた公理のなかで，$P(a)$ と書いたところがほんとうにすべての（自然数についての）性質全部に対して成立すると考えると，じつは普通簡単に証明されるように，この公理系は範疇的である．もっとくだいていえば，この公理系をみたすものは自然数以外にはありえない．すなわちニセモノは存在しないということが容易に証明できてしまう．これは美しい結果であるが，われわれの話には具合が悪い．したがってもう

ちょっと弱めて今後は $P(a)$ と書いたときに，P は変数 $a, b, c, \cdots, =, 0, ',$ $+, \dot{-}, \cdot$ と論理記号とを組み合わせてできている命題であるとする．ここに論理記号とはすでにでてきた $\neg$，$\wedge$ のほかに $\vee$（または），$\exists$（存在する），$\forall$（すべて）のことであり，このうえ $\rightarrow$ は普通の通り‘ならば’であり，$A \rightarrow B$ は $\neg A \vee B$ の略と定義し，$\leftrightarrow$ は‘同等’であり，$A \leftrightarrow B$ は $(A \rightarrow B) \wedge (B \rightarrow A)$ の略であると定義する．

さてこのように変数，$=, 0, ', \delta, +, \dot{-}, \cdot$ と論理記号で作られた命題のことを今後 formula（論理式）と呼ぶことにしよう．そして，ソックリということを自然数がみたすすべての（あるいはカナリの）formula をみたすもの，ということと定義しよう．ここでちょっと断わらなければならないのは，前の公理群のところで，

$$a=b \rightarrow b=a$$

のような形で公理を表現したが，これはじつはちょっと具合が悪い．なぜかというと，この式の意味はじつは‘任意の自然数 a, b に対してこの式が成立する’ということであって，任意の自然数 a, b についてというのがハッキリ書いてないのに了解事項になっているからである．だから今後はそれをはっきり書いて

$$\forall x \forall y (x=y \rightarrow y=x)$$

のような形に全部書きこんだものだけを公理としてとりあげることにする．

ニセモノの存在

さて論理学の定理を引用して，まず一般論としてニセモノの存在を証明することにする．そのためにまず論理学の定義を 2，3 することにする．

定義　$A_0, \cdots, A_n$ をある公理群とするときこの公理群が無矛盾であるとは

$A_0 \wedge \cdots \wedge A_n \rightarrow 0 \neq 0$ が論理だけから証明されない

ことをいう．

無限の公理群 $A_0, A_1, A_2, \cdots$ が無矛盾であるというのは，どれだけたくさんの有限部分公理群 $A_0, \cdots, A_n$ をとってきても，$A_0, \cdots, A_n$ が無矛盾である

ことをいう.

定義 数学的構造 $\mathfrak{S}$ と公理群 $A_0, A_1, \cdots$ があたえられたとき, $\mathfrak{S}$ がこの公理群のモデルであるとは, この公理群のなかのどんな公理 A_i をとっても, A_i が $\mathfrak{S}$ のなかでみたされていることをいう.

この無矛盾とモデルについてはつぎの定理が成立する.

定理 1 $\mathfrak{S}$ が $A_0, A_1, \cdots$ のモデルであれば, この公理系は無矛盾である.

(証明) もし $A_0, \cdots, A_n$ が $\mathfrak{S}$ でみたされていて,

$$A_0 \wedge \cdots \wedge A_n \rightarrow 0 \neq 0$$

が論理だけから証明されるならば, $0 \neq 0$ は $\mathfrak{S}$ でみたされていなければならない. これは矛盾である.

この定理の逆が completeness theorem (完全性定理) と呼ばれる有名な定理であり, ロジックの最初の定理らしい定理といってよいだろう.

定理 2 $A_0, A_1, \cdots$ が無矛盾な公理系であるとき, $A_0, A_1, \cdots$ のモデルとなる数学的構造 $\mathfrak{S}$ が存在する.

ここではこの定理の証明はしないで, この定理を用いてニセモノの存在を証明する. まず $A_0, A_1, \cdots$ を自然数全体によってみたされるすべての公理を並べたものであるとする. ここに自然数によってみたされる公理のなかにはペアノの公理群から証明できないものがたくさんあることを注意しておく.

さてニセモノの存在, すなわちこの $A_0, A_1, \cdots$ を全部みたしているが, 自然数全体とはまったく異なるものを作るためにまったく新しい記号 ω を導入して

$$0 \neq \omega, \ 1 \neq \omega, \ 2 \neq \omega, \cdots$$

$$A_0, A_1, A_2, \cdots$$

なる公理群を考えることにする. この新しい公理群は無矛盾である. なぜならば, もし無矛盾でないとすれば,

$0 \neq \omega, \cdots, m \neq \omega$ なる有限個の公理と

$A_0, \cdots, A_n$ なる有限個の公理が存在して

$$0 \neq \omega \wedge \cdots \wedge m \neq \omega \wedge A_0 \wedge \cdots \wedge A_n \rightarrow 0 \neq 0$$

が論理学の定理として証明されねばならない．この証明のなかで ω にすべて $m+1$ を代入すれば

$$0\neq m+1\wedge\cdots\wedge m\neq m+1\wedge A_0\wedge\cdots\wedge A_n\rightarrow 0\neq 0$$

が論理学の定理として証明される．ところで $0\neq m+1, \cdots, m\neq m+1, A_0, \cdots, A_n$ はすべて自然数全体によってみたされているから矛盾する．

さてわれわれの新しい公理群が無矛盾であることが証明された．ゆえに定理2によりこの新しい公理群をみたす数学的構造 $\mathfrak{S}$ が存在する．この $\mathfrak{S}$ を考えてみると $\mathfrak{S}$ は $A_0, A_1, \cdots$ をみたすから自然数全体とまったく同じ性質をみたすわけである．ところが反面 $\mathfrak{S}$ はまた

$$0\neq\omega,\ \ 1\neq\omega, \cdots$$

をすべてみたすから，$\mathfrak{S}$ には $0, 1, 2, \cdots$ 以外の ω なる元が入っている．したがって $\mathfrak{S}$ は自然数全体とはまったく異なった存在であり，自然数全体とソックリなニセモノである．

以上が論理学の定理を用いてのソックリなニセモノの存在証明である．この証明の具合が悪いのはこのソックリなニセモノの数学的な性質がよくわからないということである．たとえば $\omega\dot{-}1, \omega\dot{-}2, \omega\dot{-}3, \cdots$ がすべての $0, 1, 2, \cdots$ より大きいことはすぐわかるが，いったい $0, 1, 2, \cdots$ とこの $\omega\dot{-}1, \omega\dot{-}2, \cdots$ の間の数学的構造が加法と乗法とに関してどのような形をもっているか？ などは一向にわかっていない．いくつか論文があって一時は流行であったが，正直にいってあまり見通しのよい結果はないようである．念のためにいっておくが，上に作ったような $\mathfrak{S}$ のことを自然数論の nonstandard モデルといい，もともとのほんとうの自然数全体のことを standard モデルというのである．

代数的なソックリなニセモノ

さて論理学の一般論からのニセモノはまったくソックリではあるが，われわれには存在証明があるだけで，じつはあまり作ったという気がしないものであり，何とも一向にサッパリしない．もっと実際にどんなものかよくわか

っていると思えるニセモノを作ってみたいものである．しかしながらソックリというのをあまり強くとると実際には無理な注文になってしまう．ここではソックリの方をやや大目に見て，代数的な構造でニセモノを作ることにする．

さてソックリはどの程度弱めたらよいだろうか？　ここでは 1),2),3) の性質だけにかぎって，さらに 3) の数学的帰納法については，そのなかの formula $P(a)$ の P のなかには $\forall$ や $\exists$ が 1 つも現われないということにする．このように弱い意味に直された意味でのソックリなニセモノを作ることにする．

さて目的の構造を M_0 と書くことにする．まず M_0 の定義を順々にしていくことにしよう．

M_0 の定義

a） M_0 はつぎの形の t の fractional polynomial の全体であるとする．

$$a_p t^{\frac{p}{q}} + a_{p-1} t^{\frac{p-1}{q}} + \cdots + a_1 t^{\frac{1}{q}} + a_0$$

ここに p, q は自然数で $q \neq 0$ であり，$a_1, \cdots, a_p$ は実の代数的数であるとする．そのうえに $p \neq 0$ のときは $a_p > 0$ である．a_0 は有理整数であってさらに $p=0$ のときは $a_0 \geq 0$ なる条件がみたされているものとする．

b） M_0 の元について，$'$，δ，$+$，$\dot{-}$，$\cdot$ をつぎのように定義する．

まず最初に 0 自身はやはり M_0 の元である．つぎに

$$\left(a_p t^{\frac{p}{q}} + \cdots + a_0\right)' = a_p t^{\frac{p}{q}} + \cdots + a_1 t^{\frac{1}{q}} + (a_0 + 1)$$

と定義し，M_0 の 2 つの元の加法と乗法とは普通の fractional polynomial の加法と乗法によって定義する．加法と乗法との結果がふたたび M_0 の元になることは明らかであろう．

δ については，まず $p > 0$ のときには

$$\delta\left(a_p t^{\frac{p}{q}} + \cdots + a_0\right) = a_p t^{\frac{p}{q}} + \cdots + a_1 t^{\frac{1}{q}} + (a_0 - 1)$$

と定義して，$p=0$ のとき，すなわち a_0 だけのときは $\delta(a_0)$ は自然数のと

きの $\delta(a_0)$ と同じものとする．

つぎに $\dot{-}$ を定義するために $\alpha, \beta \in M_0$ を

$$\alpha = a_p t^{\frac{p}{q}} + \cdots + a_0, \quad \beta = b_l t^{\frac{l}{q}} + \cdots + b_0$$

とする．ここに q を同じにとったのは，もし α, β に現われる t のベキの分母が異なっていれば公倍数をとって同じ分母のものに書き直すことができるからである．

われわれは $\alpha \dot{-} \beta$ をつぎのごとくに定義する．

$\alpha - \beta$ を fractional polynomial として計算して結果が M_0 の元になればそれを

$$\alpha \dot{-} \beta$$

として定義する．もし結果が M_0 の元にならなければ

$$0$$

と定義する．

以上によって M_0 は完全に定義されたが，この M_0 が 2.1)—2.9) をみたすことは明らかであろう．また M_0 が自然数全体とは異なる構造であることも明らかであろうから，われわれが証明しなければならないことは M_0 が $\forall$ や $\exists$ を1つも含まない数学的帰納法をみたすということである．このために別な代数的構造を考えることにする．

K を実閉体として，K_t をつぎの形の t の fractional power series の全体とする．

$$a_p t^{\frac{p}{q}} + \cdots + a_0 + a_{-1} t^{\frac{-1}{q}} + a_{-2} t^{\frac{-2}{q}} + \cdots$$

ここに $a_p, \cdots, a_0, a_{-1}, \cdots$ は K の元であり，p, q は自然数で $q > 0$ であるとする．正のベキは高々有限個であり（1 つもなくてもよい），負のベキは無限にあってもかまわない．

つぎの代数学の定理を証明なしで用いる．

定理 3　K_t は実閉体である．

さて K_t の部分環 R_0 をつぎのごとく定義する．

R_0 の元はつぎの形の K_t の元で a_0 が有理整数であるものとする．

$$a_p t^{\frac{p}{q}} + \cdots + a_0$$

さて K_t の線型順序は普通の通りに定義される．前にのべた M_0 はちょ

うど R_0 の元で負でないものの全体になっていることは容易にわかるであろう．

いま M_0 にも大小の関係を導入することにして，

$$\alpha \leq \beta$$

を

$$\alpha \dot{-} \beta = 0$$

によって定義することにする．これが M_0 の上の線型順序になっていることは明らかであろう．

いま実数 a に対して $[a]$ はその Gauss の記号，すなわち a を超えない最大整数として，K_t の元 a について $\langle a \rangle$ を

$$a = a_p t^{\frac{p}{q}} + \cdots + a_0 + a_{-1} t^{\frac{-1}{q}} + a_{-2} t^{\frac{-2}{q}} + \cdots$$

$$\langle a \rangle = a_p t^{\frac{p}{q}} + \cdots + a_1 t^{\frac{1}{q}} + [a_0]$$

と定義する．

つぎの定理は明らかであろう．

定理 4 a が K_t の元であれば，$\langle a \rangle$ は R_0 の元であって

$$\langle a \rangle - 1 < a < \langle a \rangle + 1$$

さてわれわれはいよいよ M_0 が $\forall$ や $\exists$ を含まない数学的帰納法をみたすことを証明するのであるが，実際にはやや強い形として

$$*) \qquad A(0) \wedge \forall x (A(x) \to A(x')) \to A(a)$$

をみたすことを証明する．ここに $A(a)$ のなかには $\forall$ や $\exists$ はないものとする．M_0 がこれをみたすことをいうのであるから $A(a)$ のなかの a やそのほかの変数はすべて M_0 の元であると思ってよい．したがって $A(x)$ は変数 x と $0, ', \delta, +, \dot{-}, \cdot, =, \wedge, \vee, \neg$ と M_0 の元だけからできているものと思ってよい．いま $'$ を $+1$ でおきかえ，δ を $\dot{-}1$ でおきかえ，さらに $B(a \dot{-} b)$ を $(a > b \wedge B(a-b)) \vee (a \leq b \wedge B(0))$ でおきかえ，$a = b$ を $\neg(a < b \vee b < a)$ でおきかえればよいから $A(x)$ は

$$f(x) < g(x)$$

なる形の式から $\neg, \wedge, \vee$ によってできたものと思ってよい．ここに $f(x)$,

$g(x)$ はともに M_0 の元を係数とした x の多項式である．ここに多項式の係数は $-ax^k$ というように $-$ が入ったものも許すものとする．この意味で $f(x)<g(x)$ は容易に

$$0<f(x)$$

なる形に還元することができる．

さて $f(x)$ の係数は $\pm$ をつけたうえで M_0 の元であるから K_t の元である．K_t は実閉体であるから $f(x)$ の根を重根を含めて並べて

$$\alpha_1\leq\cdots\leq\alpha_n$$

とすれば $f(x)$ は x が K_t の元を走るとき $f(x)$ の符号は $\alpha_1,\cdots,\alpha_n$ のところでだけ変化する．したがって $0<f(x)$ は

$$x<\alpha_i,\quad \alpha_i<x<\alpha_{i+1},\quad \alpha_i<x$$

のいくつかを $\vee$ で結んだものと同等である．

いま x を K_t の特別な場合として R_0 の元だけを動くものとすれば，

$$x<\alpha$$

は
$$x<\langle\alpha\rangle \text{ または } x<\langle\alpha\rangle+1$$

のいずれかと同等であり，同様にして

$$\alpha<x$$

は
$$\langle\alpha\rangle<x \text{ または } \langle\alpha\rangle-1<x$$

のいずれかと同等である．

したがって x が R_0 の元を走るかぎり $A(x)$ は $x<\beta$ または $\gamma<x$ なる形の式から $\rightarrow,\vee,\wedge$ を用いてできたものと思ってよい．ここに β,γ は R_0 の元である．

さてこのように還元したあとで，$A(0)$ が正しく，　$A(x)$ が M_0 のある元 x で偽であったとする．$A(x)$ は $x<\beta,\gamma<x$ なる形の有限個の式から $\rightarrow,\vee,\wedge$ だけで作られているから，その真偽は有限個の R_0 の元 $\alpha_1<\cdots<\alpha_n$ をとってきて x がその $\alpha_1,\cdots,\alpha_n$ のどの間に入るかだけである．したがって M_0 の元 α_0 で　$A(\alpha_0)$ が偽になるような最小の α_0

が存在しなければならない．ところで $\alpha_0 \neq 0$ であるから α_0-1 もやはり M_0 の元である．α_0 の最小性から $A(\alpha_0-1)$

がでてくるが，これと $\forall x(A(x) \rightarrow A(x'))$

から $A(\alpha_0)$

がでてきて，$A(\alpha_0)$ が偽であることに矛盾する．

理論の応用とあとがき

さていまわれわれは M_0 が自然数全体とかなりよく似たニセモノであることを証明した．この M_0 は前の論理学の定理から導かれた構造とは異なってわれわれによく知られた構造であるからいろいろと便利なことが多い．

まず最初に 1),2),3) において P が $\forall$ や $\exists$ を含まない formula と制限してできる体系を T_0 と書くことにすれば，われわれは M_0 が T_0 のモデルであることがわかったわけである．この M_0 にはいろいろ自然数全体とはかなりハッキリと異なった性質がある．すなわちニセモノのニセモノたるところが容易に露見してしまう著しい性質がある．たとえば M_0 のなかには

$$a \neq 0 \wedge b \neq 0 \wedge 2a^2 = b^2$$

をみたすものが存在する．たとえば $a=t, b=\sqrt{2}t$ とおけばよい．これはペアノの公理すなわち 1),2),3) の P に $\forall$ や $\exists$ が入っていてもかまわないと思ったものから $\rightarrow \exists x \exists y (x \neq 0 \wedge y \neq 0 \wedge 2x^2 = y^2)$

が証明できるから M_0 の著しい性質である．

さらに M_0 には $a \neq 0 \wedge b \neq 0 \wedge c \neq 0 \wedge a^3 + b^3 = c^3$

をみたす a, b, c が存在する．たとえば $a=t, b=t, c=\sqrt[3]{2}t$ とおけばよい．もちろんペアノの公理から

$$\rightarrow \exists x \exists y \exists z (x \neq 0 \wedge y \neq 0 \wedge z \neq 0 \wedge x^3 + y^3 = z^3)$$

は証明できるから，これも M_0 の著しい性質である．このようなものはほかにもいろいろと考えられるが，いま代表としてこの 2 つだけを考えることにする．M_0 が上の T_0 のモデルであることを考えるならば，つぎの定理が得られる．

定理 5　T_0 ではつぎの命題は証明できない．

$$\neg\exists x\exists y(x\neq 0\wedge y\neq 0\wedge 2x^2=y^2)$$

$$\neg\exists x\exists y\exists z(x\neq 0\wedge y\neq 0\wedge z\neq 0\wedge x^3+y^3=z^3)$$

もっとくわしくいえばペアノの公理系からこれらの定理を証明するときに数学的帰納法を行なう命題のなかの ∀ や ∃ の使用は本質的であって，とり去ることはできない．

明らかであると思っていい忘れたが定理 5 のなかの最初の命題は $\sqrt{2}$ が無理数であることを意味している．この命題が T_0 のなかで証明できないことはスコーレム（Skolem）が予想して問題として提出，それを 1963 年頃に Shepherdson（シェファードソン）が解決したのである．ここに書いたのはその Shepherdson の証明のあらましである．

ここに少しばかり筆者の意見をのべてみたい．ペアノの公理系から $\sqrt{2}$ が無理数であることを証明するのに，数学的帰納法を実行する命題のなかの ∀ や ∃ が本質的であるという定理はどちらかといえば証明論の範囲のなかに属する問題である．しかし上の証明のなかでは証明論はあまり活躍していないようである．

これはどうしたわけであろうか？

いろいろなことが考えられて，この疑問に対する答を一刀両断にみごとにやってのけるというわけにはいかなくて残念であるが，証明を見てただちに明らかであるのが，fractional polynomial とか，実閉体とかいう数学としてよく知られた構造をうまく使っているということである．しかしこれは証明論としての言訳にはあまりならないように思われる．なぜならば，この言訳自身が証明論のいままでの怠慢を何より物語っているように思われる．もう少しくわしくいうならば，証明論はいわゆる‘数学の基礎づけ’という serious な問題から出発した．そのため自然数論，実数論，集合論というような分野ばかりが，どちらかといえば，その対象の中心にあって，しかも抽象的な一般的な問題としてとらえるというところにその重点がおかれた．そして身近にあるいろいろな実際の数学の各分野についての研究は忘れ去られたよ

うなきらいがあまりにも強いのである．したがって実閉体とか， fractional polynomial とかいったときにそれをとり扱う扱い方が証明論ではあまりお膳だてができあがっていないのである．だから，代数がたくさん使ってあってどうも，というような弁解になってでてきてしまうのである．たとえば，fractional power series になると証明論ではどのような扱いがよいか？ と聞かれると筆者にはちょっと代数の方の理論を調べてみてからといいたくなるのである．（もっと具体的にいって term として infinitary expression を許すか，それとももう少し抽象的な理論にするか？）しかもそういうことを証明論の立場できちんと調べたものはいままでないように思われる．このことがまた逆にもっと大胆な野心的な証明論の問題――たとえばフェルマーの予想がペアノの公理系からは独立できないか？ ――に証明論的にとり組もうとするとにわかにオックウに感じさせる理由でもある．（何かやろうとすると基本的なたくさんのことを全部やらなければならない．目指す問題はそれらの基本的なことを全部整理したはるか先にある.）こういう具体的な研究がないことが，たとえば代数的理論についての証明論的なみごとな定理というものがない理由にもなっているように思われる．代数的理論はたいていの場合，公理系としてきわめて特殊な簡単な形をしているから，これらについての美しい簡単な定理があってもよさそうに思われる．

この頃筆者が証明論について感じているものをだいぶ書いてしまった．これはほんとうかもしれないし，またあたっていないかもしれない．しかしそういう眼で少しながめてみたいとは思っている．さて証明論から離れてロジック一般についても少し意見をのべてみたい．筆者はこの頃次第にロジックの nonstandard モデルよりは上にのべたような代数的なモデルまたは具体的なモデルの方が興味深く思われるようになってきた．もう少し上のような代数的なモデルをたくさんとりあげて研究してみるのも面白いのではないだろうか？ 筆者には整数論，代数学とロジックの間にはたくさんの具体的な問題があるように思われる．このことが，このあまりよく知られていない仕事をとりあげて紹介した理由である．

自然数論におけるある決定問題

私の専門の分野での易しい話をという注文である．私の専門分野というとまあ logic ということになろう．ところで『数学セミナー』などを見ていると，この頃はなかなか logic の啓蒙は盛んなようである．なかなかよい本も多く，いろいろ logic についての話にふれる機会も多いようである．たとえばわが親友前原昭二氏の本などは懇切丁寧で私にこれ以上のことができるとは思えない．それに，いつも，いつも，$\neg$（否定），$\wedge$（そして），$\vee$（または），$\forall$（すべて），$\exists$（存在する）のお話では聞く方もすっかりアキアキされることと思う．

ここでは，$\neg, \wedge, \vee, \forall, \exists$, については定義ぐらいは知っているものと仮定して，1 つだけ定理を証明してみることにする．予備知識はほとんど仮定しないし，logic といっても，よく知っている自然数についてであるから，順を追って読んでいけば，logic 全体についての idea を具体的な例について紹介することにもなろうかと思う．

定理自身はきわめて古く 1920 年頃かと思うがあまりきちんと証明してある本を見ないので多少の役に立つこともあろうかと思われる．

細かい説明をする前に，大ざっぱに問題を説明することにする．普通自然数では四則大小が最も重要な概念と考えられる．いま四則大小と論理記号とを結合して構成できる命題のことを算術的な命題という．まず算術的な命題

をきちんと定義するために算術についての言語の定義から始めよう．

算術の言語

算術の言語はつぎのものから構成される．

特定な自然数を表わす記号	0，1
関数記号	$+, \cdot$
大小の記号	$<, =$
論理記号	$\neg, \wedge, \vee, \forall, \exists$
自由変数	$a, b, c, \cdots$
束縛変数	$x, y, z, \cdots$
カッコ	( )

カッコは結合の順序を示すために用いるが，これは普通のカッコの用い方であるからとくに説明しない．特定の自然数を表わす記号はもちろん，0, 1, 2, 3, … と全部入れてもよいのであるが，2 は 1+1，3 は ((1+1)+1) というふうに表わされるので 0 と 1 とだけとっておくことにする．もちろんあとで 3 とか 5 とかを断わりなしに用いるが，これは上のように表わされたものとする．

自由変数 $a, b, c, \cdots$ は任意の自然数を表わす変数である．束縛変数 $x, y, z, \cdots$ は $\forall$ か $\exists$ と結びついて，$\forall x$（すべての自然数 x について）とか，$\exists x$（ある自然数 x が存在して）というふうに用いられる．

つぎに算術の term について定義しよう．

算術の term はつぎのように定義される．

1) 0 と 1 と自由変数は算術の term である．

2) t_1 と t_2 とが算術の term であるとき，(t_1+t_2) と $(t_1 \cdot t_2)$ とは算術の term である．

3) 以上の 1 と 2 によってできたもののみが算術の term である．

たとえば $(a+b)\cdot(c+d)+3$ などは算術の term である．もっともこれは正式に表わせば，まず・で結合したあとにもう 1 つカッコがいるし，3 を正式に表現して，+3 のあとでまたカッコを必要とするが，こういうことは

ここではいつも常識にしたがって省略することにする．

つぎに同じように算術の formula を定義することにする．算術の formula はつぎのごとく定義される．

1)　t_1, t_2 が算術の term であるとき，$t_1=t_2$ と $t_1<t_2$ は算術の formula である．

2)　A, B が算術の formula であるとき，$\neg A$, $A\wedge B$, $A\vee B$ は算術の formula である．

3)　$A(a)$ が算術の formula であって，$A(a)$ に入っていない任意の束縛変数 x をとるとき，$\forall xA(x)$ と $\exists xA(x)$ とはともに算術の formula である．

4)　以上の 1), 2), 3) によってできたもののみを算術の formula という．

算術の formula のなかで自由変数を含まないものを算術の命題という．

算術の formula ではいったいどの程度のことが表現できるであろうか？たとえばフェルマーの問題は巾を含むので文字通りの意味では算術の命題ではない．しかし，算術の命題によって表現される命題の範囲は意外に広く，たとえば上のフェルマーの問題と実質的に同等なものが算術の命題によって表現されることが知られている．

さて，算術の命題の決定問題というのは，1 つの算術的命題があたえられたとき，その命題が真か偽かを決定する effective な方法が存在するか？という問題を意味する．effective という意味はいまとなってはよく知られていることと思うが，記憶容量が無限であるような理想的なコンピューターにうまいプログラムをあたえて，どんな算術的な命題をあたえても，真か偽かをコンピューターが解決するようにできるか？ということだと思っていただければよい．

さて算術の決定問題は，そのような effective な方法はないという形で否定的に解決（ゲーデル）されている．これは常識的にいって当然といえる．たとえばフェルマーの問題は上にのべたように算術的命題によって表現されるから，もしそのような方法があれば，コンピューターがフェルマーの問題

を解いてくれるということになる．このような一般公式がコンピューターによってできるというのはちょっと虫がよすぎるといってよいであろう．

いま算術的 formula で・を 1 つも含まないものを加法的 formula といい，加法的 formula で自由変数を 1 つも含まないものを加法的な命題ということにする．

いまこの加法的な formula ではどのようなものが表現できるであろうか．乗法は用いてはいけないのであるが，$3\cdot a$ などは形式的には乗法でも，$a+a+a$ で表わされるから加法的 formula のなかに入っていてもよいと考えることにする．一般に n が $0,1,2,\cdots$ であるとき $n\cdot a$ の形は用いてよい．いま同じように n が $1,2,\cdots$ のとき

$$a\equiv b \pmod{n}$$

は
$$\exists x(a=n\cdot x+b \vee b=n\cdot x+a)$$

で表わすことができるので，加法的 formula のなかに入っているものと思ってよい．ここで注意すべきことは，n は $0,1,2,\cdots$ にかぎるのであって，n が変数のときは加法的 formula にはならない．（明らかな理由から以下には n が 0 か 1 のときは (mod n) は用いないことにする．）

さて，ここで加法的な命題については，決定問題が解ける，すなわち加法的な命題については，その命題が真か偽かを effective に判定する判定法が存在することを証明する．実際には判定する仕方を実際に提出してみせるのである．

われわれは加法的 formula を $t_1=t_2$ と $t_1<t_2$ から出発して構成したが，上にのべたことによって

$$t_1\equiv t_2 \pmod{n}$$

なる形も出発点の formula のなかにくり入れて加法的 formula を定義しても一向にさしつかえないので今後そのように加法的 formula の定義を拡張しておくことにする．

いくつかの補題をまずのべることにすれば

補題 1 A が加法的な formula であって，$\forall$ と $\exists$ とを 1 つももっていな

いとすれば，A は

$$(B_{11}\wedge\cdots\wedge B_{1n_1})\vee\cdots\vee(B_{m1}\wedge\cdots\wedge B_{mn_m})$$

なる形と同等である．ここに B_{ij} は $t_1=t_2$，$t_1<t_2$，$t_1\equiv t_2 \pmod n$ なる形の 1 つである．

（証明） $\vee$ と $\wedge$ についての分配律と

$$\neg(A\wedge B),\quad \neg(A\vee B)$$

がそれぞれ

$$\neg A\vee\neg B,\quad \neg A\wedge\neg B$$

に同等であることを用いることにより，A が上のような形で B_{ij} が $t_1=t_2$，$t_1<t_2$，$t_1\equiv t_2 \pmod n$ なる形かその否定の形の 1 つであるものと同等であることがわかる．ところで，

$$\neg t_1=t_2 \text{ は } t_1<t_2\vee t_2<t_1$$

$$\neg t_1<t_2 \text{ は } t_1=t_2\vee t_2<t_1$$

$$\neg(t_1\equiv t_2 \pmod n)$$

は

$$t_1\equiv t_2+1 \pmod n\vee\cdots\vee t_1\equiv t_2+(n-1) \pmod n$$

とそれぞれ同等であることがわかるから，ふたたび $\wedge$ と $\vee$ との分配律を用いることにより補題が証明される．

いま一般に $B_1\wedge\cdots\wedge B_m$ なる形の formula で B_i が，

$$t_1=t_2,\quad t_1<t_2,\quad t_1\equiv t_2 \pmod n$$

なる形の 1 つであるような formula を基本的な formula と呼ぶことにしよう．

補題 2

$$\exists x(B_1(x)\vee\cdots\vee B_m(x))$$

は

$$\exists xB_1(x)\vee\cdots\vee\exists xB_m(x)$$

に同等である．

証明省略．

定理 1　いま $B(a)$ を基本的な formula とする．いま $\exists xB(x)$ を同等な基本的な formula に変形する effective な方法があれば，加法的な命題についての決定問題は解決する．

（証明） いま加法的な formula A があたえられたとして，仮定より A と

同等な ∀ も ∃ も含まない加法的 formula を effective に求められることをまず証明する．

証明は，A のなかにある ∀ と ∃ との数の数学的帰納法による．もし A のなかに ∀ や ∃ が 1 つもなければ明らかであるから，帰納法の仮定によって A が ∀ か ∃ を 1 個だけ含む場合に証明すればよいことが容易にわかる．ところで，$\forall x$ は $\neg\exists x\neg$ で表わされるので，A が $\exists xB(x)$ の形であるときに証明すれば十分である．ところで補題 1 と 2 を用いれば，A が $\exists xB(x)$ で $B(a)$ が基本的な formula であるときに証明すればよいことがわかるが，これは定理の仮定であるから問題はない．さて定理の証明をする．いま A が加法的命題とする．いままでのべてきたことにより，A は

$$t_1=t_2,\ \ t_1<t_2,\ \ t_1\equiv t_2 \pmod n$$

なる形の formula から ∧ と ∨ とを結合させてできたものである．ところで，この formula は自由変数を 1 つも含んでいない．ゆえに，t_1, t_2 は 0 と 1 から + を何度か結合させてできたものである．すなわち 0, 1, 2, …の 1 つと思ってさしつかえない．

ところで，l, m, n がかかる 0, 1, 2, … として具体的にあたえられたときには，

$$l=m,\ \ l<m,\ \ l\equiv m \pmod n$$

の真偽は決定される．真偽が決定されている formula から ∧ と ∨ との結合によってできている formula の真偽を effective に決定できることは明らかであるから定理は証明された．

定理 2　加法的命題の決定問題は肯定的に解決される．すなわち加法的命題の真偽を決定する effective な方法が存在する．

（証明）　定理 1 により A が $\exists xB(x)$ で $B(a)$ が基本的 formula であるような A を基本的な formula に変形する effective な方法を提出してみせればよい．

いま A は

$$\exists xB(x)$$

で $B(x)$ は　$t_1(x)=t_2(x), t_1(x)<t_2(x), t_1(x)\equiv t_2(x) \pmod n$

なるたくさんの形を ∧ で結合してできたものである．ここに $t_i(x)$ は 0

と 1 と x と自由変数に + を何度か施してできたものにちがいないから，簡単な変形を施すことにより $mx+t$ の形になっていると思ってさしつかえない．ここに t は 0, 1, 自由変数に + を何度か施してできた任意の term であって x を含んでいないことが重要である．m は具体的にあたえられた $0,1,2,\cdots$ の 1 つである．

まず $t_1(x)=t_2(x)$ なるものを調べてみよう．この形はいまのべたことにより

$$mx+t=nx+s$$

の形と思ってよい．いろいろな場合に分けて考えてみると

1）$m=n$ の場合

このときは，この式は $t=s$ と同等である．いま $\exists xB(x)$ を

$$\exists x(mx+t=nx+s\wedge B_0(x))$$

というふうにわけて考えてみるとこれは順々に

$$\exists x(t=s\wedge B_0(x))$$

$$t=s\wedge\exists xB_0(x)$$

と同等になる．ゆえにわれわれの変形を $\exists xB_0(x)$ について続行すればよいから，はじめからこの形の式は 1 つも含まれていないと思ってよい．

2）$n<m$ の場合

$$(m-n)x+t=s$$

と変形する．

3）$m<n$ の場合

$$(n-m)x+s=t$$

と変形する．

同様の変形を　$t_1(x)<t_2(x)$ と $t_1(x)\equiv t_2(x)\ (\mathrm{mod}\ n)$

とに行なうことにより，$B(x)$ はつぎのようなたくさんの形を $\wedge$ で結合してできたものと思ってよい．

$$mx+s=t,\ \ mx+s<t,\ \ t<mx+s,\ \ mx+s\equiv t\ (\mathrm{mod}\ n)$$

ここで m は $1,2,3,\cdots$ の 1 つであり，n は $2,3,4,\cdots$ の 1 つであるとす

る．さて，この $B(x)$ をもっとくわしく並べて書けば

$$m_{11}x+s_{11}=t_{11},\quad m_{12}x+s_{12}=t_{12},\quad \cdots$$
$$m_{21}x+s_{21}<t_{21},\quad m_{22}x+s_{22}<t_{22},\quad \cdots$$
$$t_{31}<m_{31}x+s_{31},\quad t_{32}<m_{32}x+s_{32},\quad \cdots$$
$$m_{41}x+s_{41}\equiv t_{41} (\mathrm{mod}\ n_1),\quad m_{42}x+s_{42}\equiv t_{42} (\mathrm{mod}\ n_2),\quad \cdots$$

を $\wedge$ で結合してできたものということになる．いま k を $1,2,3,\cdots$ の 1 つとすれば

$$mx+s=t,\ \cdots,\ mx+s\equiv t (\mathrm{mod}\ n)$$

はそれぞれ

$$kmx+ks=kt,\ \cdots,\ kmx+ks\equiv kt (\mathrm{mod}\ kn)$$

と同等になるから

$$m_{11}, m_{12}, \cdots$$
$$m_{21}, m_{22}, \cdots$$
$$m_{31}, m_{32}, \cdots$$
$$m_{41}, m_{42}, \cdots$$

の最小公倍数をとることにより，適当に変形して $B(x)$ ははじめから

$$mx+s_{11}=t_{11},\ mx+s_{12}=t_{12}, \cdots$$
$$mx+s_{21}<t_{21},\ mx+s_{22}<t_{22}, \cdots$$
$$t_{31}<mx+s_{31},\ t_{32}<mx+s_{32}, \cdots$$
$$mx+s_{41}\equiv t_{41}\ (\mathrm{mod}\ n_1),\ mx+s_{42}\equiv t_{42}\ (\mathrm{mod}\ n_2), \cdots$$

を $\wedge$ で結合してできたものであるとしてよい．このとき $\exists xB(x)$ は明らかに

$$\exists yC(y)$$

と同等になる．ここに $C(y)$ は

$$y+s_{11}=t_{11},\ y+s_{12}=t_{12}, \cdots$$
$$y+s_{21}<t_{21},\ y+s_{22}<t_{22}, \cdots$$
$$t_{31}<y+s_{31},\ t_{32}<y+s_{32}, \cdots$$
$$y\equiv 0\ (\mathrm{mod}\ m),\ y+s_{41}\equiv t_{41}\ (\mathrm{mod}\ n_1), \cdots$$

を $\wedge$ で結合してできたものである．したがってわれわれは $B(x)$ がはじめから

$$x+s_{11}=t_{11},\quad x+s_{12}=t_{12},\cdots$$

$$x+s_{21}<t_{21},\cdots$$

$$t_{31}<x+s_{31},\cdots$$

$$x+s_{41}\equiv t_{41}(\mathrm{mod}\ n_1),\cdots$$

なる形を $\wedge$ で結んでできたものと思ってよい．

さて，勝手な u について

$$x+s=t,\ \cdots,\ x+s\equiv t(\mathrm{mod}\ n)$$

はそれぞれ　$x+s+u=t+u,\ \cdots,\ x+s+u\equiv t+u(\mathrm{mod}\ n)$

と同等であるから

$$s_{11}+s_{12}+s_{13}+\cdots+s_{21}+\cdots+s_{31}+\cdots+s_{41}+\cdots$$

を s とおき　$t'_{11}=t_{11}+s,\cdots$

とおけば $B(x)$ は

$$x+s=t'_{11},\cdots$$

$$x+s<t'_{21},\cdots$$

$$t'_{31}<x+s,\cdots$$

$$x+s\equiv t'_{41}\ (\mathrm{mod}\ n_1),\cdots$$

を $\wedge$ で結合したものと思ってよく，したがって，$\exists xB(x)$ はつぎの

$$\exists y((s<y\vee s=y)\wedge C(y))$$

に同等である．ここに $C(y)$ は

$$y=t'_{11},\cdots$$

$$y<t'_{21},\cdots$$

$$t'_{31}<y,\cdots$$

$$y\equiv t'_{41}\ (\mathrm{mod}\ n_1),\cdots$$

を $\wedge$ で結合したものである．

$$\exists y((s<y\vee s=y)\wedge C(y))$$

は　$\exists y(s<y\wedge C(y))\vee\exists y(s=y\wedge C(y))$

に同等であるから，問題はこの $\vee$ で結ばれた 2 つの formula に還元される．ゆえにわれわれは $B(x)$ が初めから

$$x=t_{11},\cdots$$

$$x<t_{21},\cdots$$

$$t_{31}<x,\cdots$$

$$x\equiv t_{41}\pmod{n_1},\cdots$$

の形を $\wedge$ で結合したものと思ってよい．いまもし $B(x)$ が $x=t$ なる形を1つでも含むとして

$$(x=t)\wedge C(x)$$

なる形であるとすれば，$\exists xB(x)$ は $C(t)$ と同等になり定理は証明されたことになる．ゆえに $B(x)$ ははじめからつぎのものの $\wedge$ による結合としてよい．

$$x<s_1,\ x<s_2,\cdots,\ x<s_k$$

$$t_1<x,\ t_2<x,\cdots$$

$$x\equiv u_1\pmod{n_1},\cdots$$

さて，$(i_{11},i_{12},\cdots,i_{1k})$，$(i_{21},i_{22},\cdots,i_{2k})$，$\cdots$ を $1,2,\cdots,k$ のすべての順列とすれば

$$(s_{i_{11}}\leq s_{i_{12}}\leq\cdots)\vee(s_{i_{21}}\leq s_{i_{22}}\leq\cdots)\vee\cdots$$

はつねに成立するので $\exists xB(x)$ は

$$\exists x((s_{i_{11}}\leq s_{i_{12}}\leq\cdots)\wedge B(x))\vee\exists x((s_{i_{21}}\leq s_{i_{22}}\leq\cdots)\wedge B(x))\vee\cdots,$$

と同等であり，

$$\exists x((s_{i_{11}}\leq s_{i_{12}}\leq\cdots)\wedge B(x))$$

は

$$(s_{i_{11}}\leq s_{i_{12}}\leq\cdots)\wedge\exists xC(x)$$

と同等である．

ここに $C(x)$ はつぎのものの $\wedge$ による結合である．

$$x<s_{i_{11}}$$

$$t_1<x,\quad t_2<x,\cdots$$

$$x\equiv u_1\pmod{n_1},\cdots$$

同様のことを t についても行なうことによりわれわれははじめから $B(x)$ はつぎの形の $\wedge$ による結合と思ってよい．

$$x<s,\quad t<x,$$

$$x\equiv u_1\pmod{n_1},\quad\cdots,\quad x\equiv u_k\pmod{n_k}$$

いま $n_1, n_2, \cdots, n_k$ の最小公倍数を n としよう．このとき $\exists x B(x)$ は $C_1 \vee \cdots \vee C_n$ と同等である．ここに $C_m (1 \leq m \leq n)$ は

$$t+m<s,\ t+m \equiv u_1 (\bmod\ n_1),\ \cdots,\ t+m \equiv u_k (\bmod\ n_k)$$

を $\wedge$ で結合してできたものである．この同等性はほとんど明らかであるので，演習問題としておきたい．

いまここに $t<x$ なる形が必ずあるものとしたが，もし $t<x$ が全然ない場合には，$\exists x B(x)$ は　　　$C_0 \vee \cdots \vee C_{n-1}$

と同等であって，ここに $C_m (m<n)$ は

$$m<s,\ m \equiv u_1 (\bmod\ n_1),\ \cdots,\ m \equiv u_k (\bmod\ n_k)$$

を $\wedge$ で結合してできたものとすればよい．

いずれにしても，$C_1 \vee \cdots$ または $C_0 \vee \cdots$ はそれぞれ $\forall$ や $\exists$ を含まない加法的 formula であるので定理の証明は終った．

この定理は考え方によっては算術における乗法の重要性を証明したものと思ってもよいし，また加法だけで表現できる formula がいかに弱いか，またその表現能力の範囲が $=, <, \equiv (\bmod\ n)$ から $\wedge$ や $\vee$ で結合したもの以上の能力がないことを証明したといってよい．しかし，変形の操作が effective であることがまた大切なところである．

ちなみに 1920 年頃この問題が解けた頃は，もうちょっと工夫すれば乗法を含む formula についても同様なことができると思ったようである．このことが否定的に解決されたことは，前にのべた通りである．残念ながら，最初に証明した人の名前は覚えていないし，正直にいうとその論文も見たこともない．

ゲーデルの新しい公理について

1970 年に集合論の世界にちょっとした突発事件が起きそうで起きなかった．これが将来において集合論の様相をすっかりかえてしまうような大爆発になるのか，それとも大洋の一角の小さな火山島を吹き上げたくらいに留まるのかいまのところは全然わからないが，結果は将来のお楽しみということにして現在までのところについてのべてみたい．

事柄は簡単でゲーデルがタルスキーに Proceeding of National Academy of Science にだす原稿の草稿として 5 ページになるメモを送ったのであり，その title は 'Some considerations leading to the probable conclusion that the true power of the continuum is $\aleph_2$' というのである．

ところで，このメモは論文の下書きというようなものではなく，定義なども全然ハッキリせず，順序，体裁などもまったくのデタラメで落書きに近いまったくのメモである．どうしてこういう原稿をタルスキーに送ったのかよくわからないが，(タルスキー，クリーネ，ゲーデルが現在 logician でアカデミーの会員であるから，Proceedingにだすべくタルスキーに送るのは当然だが，こんなにヒドイ原稿を送ったということがよくわからない.） まあ考えようによっては論文を読んでチェックしてくれるのには適任であり，悪く考えると読んでわかったらタルスキーがわかり易くきちんと書き直してくれることを期待したのかもしれない．ゲーデルがタルスキーを下請に選んだと

思うとちょっと面白いが，これは人の悪い想像かもしれない．ところでタルスキーにはこれは全然わからない．それでタルスキーが近い側近達にまわしたが全然わからないというのが事の始まりである．私も読んでみたがよくわからない．タルスキーに近い C.C. Chang から小生への私信によれば（1970年夏），いままでわかったという人がいないとのことである．私は 1970 年の夏ゲーデルに電話をかけて聞いてみた．できれば，定義でちょっと不明なところなどを確かめたかったのである．ゲーデル先生の返事ではアレハ間違いがあるから，そのうち直したら原稿を送ってあげる，とのことであった．これでその話は打切りになって雑談にかわってしまった．ところで小生がわからなかったのは正しい間違っているなどというところよりずっと以前の基本的な定義に関することだったが，ゲーデル先生にああいわれてはそれ以上に追求するわけにはいかなかった．だいたい‘間違いがある’というのがほんとうに serious な間違いなのか，電話で質問されるのが煩しくてちょっとした間違いを口実に逃げたのかその辺もよくわからない．とにかくいままでのところは訂正した原稿を私は受けとっていないし，私自身はこのつぎ会うときまではまあ仕方がないと諦めている．

この原稿がでるまでにはこの事柄がずっと進展していてもっと正確なことがわかっているということもありうるが，また当分の間このままということも考えられる．ここに一応の紹介をしたい．

Pantachie

ゲーデルの仕事はある意味で Hausdorff（ハウスドルフ，1868—1942）の仕事の継承であるから，まず 1910 年頃の Hausdorff の仕事についてのべたい．

いま実数の点列 $A=(a_0, a_1, a_2, \cdots, a_n, \cdots)$ について考えよう．ここに n は自然数を走り，a_n はすべて実数であるものとする．このような実数の点列 A, B があたえられたときに（すなわち $B=(b_0, b_1, b_2, \cdots)$ とするとき）

$$A \sim B$$

を‘十分大きい自然数 n_0 をとると，すべての自然数 n について $n \geq n_0$ ならば $a_n = b_n$’ということと定義する．もし論理記号を用いるならば

$$\exists n_0 \forall n \geq n_0 (a_n = b_n)$$

のことである．

たとえば　　$(0,0,1,1,1,\cdots) \sim (1,1,1,1,1,\cdots)$

となる．

同様にして　　$A < B$

を‘十分大きい n_0 をとったとき，すべての $n \geq n_0$ について $a_n < b_n$ が成立する’ことと定義する．もし論理記号を用いるならば

$$\exists n_0 \forall n \geq n_0 (a_n < b_n)$$

のことである．

たとえば　　$(1,1,0,0,0,\cdots) < (0,0,1,1,1,\cdots)$

となる．もちろん簡単な性質として

$$A \sim A$$

$$A \sim B \rightarrow B \sim A$$

$$A \sim B, B \sim C \rightarrow A \sim C$$

$$A \sim A_1, B \sim B_1, A < B \rightarrow A_1 < B_1$$

$$A < B, B < C \rightarrow A < C$$

$$A \sim B \rightarrow \neg (A < B)$$

が成立する．ここに $\neg (A < B)$ は‘$A < B$ でない’を表わすのは普通の通りである．

もちろん $A < B, B < A, A \sim B$ のいずれもみたさない A, B は容易に見つかる．たとえば　　$(0,1,0,1,\cdots)$ と $(1,0,1,0,\cdots)$

をとればよい．

Hausdorff のアイディアはこの実数の点列のうまい集合を考えて，それが $<$ によって線型順序になっているようにして，それがある意味で直線連続体の拡張になっているようにしようということであり，ゲーデルの場合はそのような超直線連続体に普通の人が直線連続体に感じるような直観をもって

いるようであって，彼はそういうような私にとってはスーパーマンの直観をもって新しい公理を提出するのである．

話をくわしく説明するために，Hausdorff が P. Du Bois-Reymond の実関数についての定義から導いた Pantachie というものの定義をする．

いま実数の点列の集合 $\mathfrak{F}$ を考えよう．すなわち $A \in \mathfrak{F}$ であれば A は実数の点列である．

$\mathfrak{F}$ が線型であるということを‘$\mathfrak{F}$ から相異なる 2 点 A, B をとってきたときに $A \lessdot B$ か $B \lessdot A$ が成立する’ということと定義する．すなわちもし論理記号を用いるならば

$$\forall A, B \in \mathfrak{F} (A \lessdot B \vee A = B \vee B \lessdot A)$$

ここに $\forall$ は‘すべて’，$\vee$ は‘または’を表わす論理記号である．

線型な $\mathfrak{F}$ はきわめて特殊な性質をもっている．たとえばもし $\mathfrak{F}$ から A, B をとってきて $A \sim B$ であれば，$A = B$ である．

すなわち $\mathfrak{F}$ が線型ならば

$$A \in \mathfrak{F}, B \in \mathfrak{F}, A \sim B \rightarrow A = B$$

がみたされる．

線型な $\mathfrak{F}$ の例としてはたとえば，a が任意の実数を動くときに $(a, a, a, \cdots)$ なる点列の全体をとれば，これが線型になっていることは明らかであろう．

Hausdorff の Pantachie は‘極大な線型な点列の集合’として定義される．すなわち点列の集合 $\mathfrak{P}$ が Pantachie であるとは

1)　$\mathfrak{P}$ は線型である．

2)　どんな線型な $\mathfrak{F}$ をとってきても $\mathfrak{P} \subseteq \mathfrak{F}$ ならば，$\mathfrak{P} = \mathfrak{F}$ が成立する．

の 2 つの条件がみたされることをいう．

Pantachie が存在することは，選択公理か Zorn の補題を用いれば明らかである．さらに実数の点列 A がはじめにあたえられているときには，A を含むような Pantachie が存在することも明らかである．いま互いに比較可能ではない無限に多くの‘実数の点列’が存在するから無限に多くの異なった

Pantachie が存在することは明らかである．

Hausdorff はこの Pantachie が超直線連続体のよき候補，すなわち直線連続体に類似の性質をもっていることを指摘したのである．もっとくわしくいうならば直線連続体と $\boldsymbol{\omega}$ との関係が，この Pantachie と $\boldsymbol{\omega}_1$ との関係にやや似ていることを指摘したのである．さて最初に Pantachie の濃度はどれだけであろうか？　正確な濃度はただちにはわからないが，上界だけは簡単に求まる．すべての実数の点列の集合の濃度は

$$\overline{\overline{(2^{\omega})^{\omega}}}=\overline{\overline{2^{\omega\times\omega}}}=\overline{\overline{2^{\omega}}}$$

であり，Pantachie はその部分集合であるから濃度が高々連続体の濃度であることはたしかである．

Pantachie の基本的性質

いま Pantachie の性質を調べるために 1 つの Pantachie $\mathfrak{P}$ を固定して，$\mathfrak{P}$ の部分集合を，$\mathfrak{S}$ や $\mathfrak{T}$ で表わすことにする．いま

$$\mathfrak{S}<\mathfrak{T}$$

を‘すべての $\mathfrak{S}$ の点 A とすべての $\mathfrak{T}$ の点 B とについて $A<B$ が成立する’ことと定義する．　　$A\in\mathfrak{S},\, B\in\mathfrak{T} \rightarrow A<B$

が成立することである．

いま $\mathfrak{P}$ の任意の点 A をとったとき

$\mathfrak{S}<A$ は $\forall B\in\mathfrak{S}(B<A)$ のこと，

また　$A<\mathfrak{T}$ は $\forall B\in\mathfrak{T}(A<B)$ のこと，

と定義する．

定理 1　$\mathfrak{S}$ が高々可付番ならば $\mathfrak{S}<A, B<\mathfrak{S}$ なる A, B が $\mathfrak{P}$ のなかに存在する．またさらに $\mathfrak{S}$ と $\mathfrak{T}$ とが可付番で $\mathfrak{S}<\mathfrak{T}$ であれば $\mathfrak{S}<C<\mathfrak{T}$ なる C が $\mathfrak{P}$ のなかに存在する．

（証明）　$\mathfrak{S}$ は高々可付番であるから，その元を並べて

$$S_0=(s_{00}, s_{01}, s_{02}, \cdots)$$

$$S_1=(s_{10}, s_{11}, s_{12}, \cdots)$$

$$S_2=(s_{20}, s_{21}, s_{22}, \cdots)$$
$$\vdots$$

としてよい．いま $x_0, x_1, \cdots$ をつぎのように順々にとることにする．

$$s_{00}<x_0$$
$$s_{01}, s_{11}<x_1$$
$$s_{02}, s_{12}, s_{22}<x_2$$
$$\vdots$$

いま
$$X=(x_0, x_1, x_2, \cdots)$$
とおけば，$X\in\mathfrak{P}$ はわからないが，
$$\mathfrak{S}<X$$
は明らかであろう．いまもし $\mathfrak{S}<A$ なる $\mathfrak{P}$ の元 A が存在しないとすれば，$\mathfrak{P}\cup\{X\}$ は線型となり，これは $\mathfrak{P}$ の極大性に反する．ゆえに $\mathfrak{S}<A$ なる $\mathfrak{P}$ の元 A が存在する．

$B<\mathfrak{S}$ なる B の存在も同様にして証明することができる．

つぎに
$$\mathfrak{S}<\mathfrak{T}$$
を仮定して $\mathfrak{S}<C<\mathfrak{T}$ なる C が $\mathfrak{P}$ のなかにあることを証明しよう．$\mathfrak{S}<A$ なる A が $\mathfrak{P}$ のなかにあることを証明したときと同じように $\mathfrak{S}<X<\mathfrak{T}$ なる X が（$\mathfrak{P}$ のなかでなくても）存在することを証明すれば十分である．いま $\mathfrak{T}$ も高々可付番であるから，これを並べて

$$T_0=(t_{00}, t_{01}, t_{02}, \cdots)$$
$$T_1=(t_{10}, t_{11}, t_{12}, \cdots)$$
$$T_2=(t_{20}, t_{21}, t_{22}, \cdots)$$
$$\vdots$$

とする．いま自然数列 $n_0<n_1<n_2<\cdots$ を上手に選べば

$$n_0\leq n \rightarrow s_{0n}<t_{0n}$$
$$n_1\leq n \rightarrow s_{0n}, s_{1n}<t_{0n}, t_{1n}$$
$$n_2\leq n \rightarrow s_{0n}, s_{1n}, s_{2n}<t_{0n}, t_{1n}, t_{2n}$$
$$\vdots$$

であるようにできる．いま $x_0, x_1, x_2, \cdots$ を上手に選んで

$$n_0 \leq n < n_1 \rightarrow s_{0n} < x_n < t_{0n}$$

$$n_1 \leq n < n_2 \rightarrow s_{0n}, s_{1n} < x_n < t_{0n}, t_{1n}$$

$$n_2 \leq n < n_3 \rightarrow s_{0n}, s_{1n}, s_{2n} < x_n < t_{0n}, t_{1n}, t_{2n}$$

$$\vdots$$

が成立するようにできる．いま

$$X = (x_0, x_1, x_2, \cdots)$$

とおけば，
$$\mathfrak{S} < X < \mathfrak{T}$$
は明らかである．

このことからただちに明らかなのは $\mathfrak{P}$ の点 $A_0, A_1, A_2, \cdots$ と A をとるとき $A_0 < A_1 < A_2 < \cdots \rightarrow A$ とか $A_0 > A_1 > A_2 \cdots \rightarrow A$ とかは絶対に起こりえないことである．

定理 2 $\mathfrak{P}$ の濃度は連続体の濃度に等しい．

（証明） 前に $\mathfrak{P}$ の濃度が高々連続体の濃度であることを証明したから，こんどは少なくとも連続体の濃度であることを証明すればよい．

まず第 1 にすべての有理数を並べて

$$r_0, r_1, r_2, \cdots$$

とする．いま $\mathfrak{P}$ の点 $A_0, A_1, A_2, \cdots$ をつぎのように順々にとっていくことにする．

1) A_0 は勝手にとることにする．

2) $A_0, \cdots, A_n$ までとったとき，A_{n+1} を $A_0, \cdots, A_{n+1}$ の $<$ についての順序関係がちょうど $r_0, \cdots, r_{n+1}$ の大小関係と同じになっているようにとる．

たとえば $n=2$ のとき $r_0 < r_3 < r_2 < r_1$ ならば A_3 を A_0 と A_2 との間にとるのである．もちろんこの場合 A_0, A_1, A_2 は帰納法の仮定により $A_0 < A_2 < A_1$ であるように選ばれている．

いまこのように $A_0, A_1, A_2, \cdots$ がすべて選ばれたとする．いま任意の実数 x があたえられたとき，この x に対応する $\mathfrak{P}$ の元 X を定めるためにつ

ぎのように $\mathfrak{S}$ と $\mathfrak{T}$ とを定義する．

$$\mathfrak{S}=\{A_n \mid r_n \leq x\}$$

$$\mathfrak{T}=\{A_n \mid x < r_n\}.$$

もちろん $\mathfrak{S}$ も $\mathfrak{T}$ も可付番で，　$\mathfrak{S}<\mathfrak{T}$

は明らかであろう．したがって前定理により，

$$\mathfrak{S}<X<\mathfrak{T}$$

なる X が $\mathfrak{P}$ のなかに存在する．このような X を 1 つ選んで x に対応させる．これはすべての実数から $\mathfrak{P}$ のなかへの 1 対 1 の対応になっていることは明らかであるから，$\mathfrak{P}$ の濃度が少なくとも連続体の濃度であることが証明された．

定理 1 のもう 1 つの応用として $A_0<A_1<\cdots<A_\alpha<\cdots$ $(\alpha<\omega_1)$ なる上昇列を $\mathfrak{P}$ のなかでつぎのように超限帰納法で定義することができる．

1)　A_0 は任意にとる．

2)　$A_0<\cdots<A_\beta<\cdots$ $(\beta<\alpha)$ が定義されたとき，$\mathfrak{S}=\{A_\beta \mid \beta<\alpha\}$ とおけば $\alpha<\omega_1$ であるから $\mathfrak{S}$ は高々可付番，ゆえに $\mathfrak{S}<A$ なる A が存在する．その 1 つを A_α と定義する．

同様にして $A_0>A_1>\cdots>A_\alpha>\cdots$ $(\alpha<\omega_1)$ なる下降列も定義することができる．問題は ω_1 から先どこまでいくことができるかということである．これについてはつぎに少しのべてみることにする．

Hausdorff の公理

つぎのものは Hausdorff が公理として主張したものではないが，Hausdorff がとりあげて考えゲーデルがしばしば Hausdorff の連続性公理と呼んだりするので，ここでは Hausdorff の公理と呼ぶことにする．まずアイディアを端的にいうと，超連続体と呼ぶにふさわしいものが Pantachie のなかに存在するということである．もう少しハッキリいうと，直線連続体と ω との関係が，超連続体と ω_1 との関係になっているような超連続体が存在することを

いうものである．

〈Hausdorff の公理〉

Pantachie $\mathfrak{P}$ でつぎの条件をみたすものが存在する．

1) $A_0 < A_1 < \cdots < A_\alpha < \cdots$ $(\alpha < \omega_2)$ なる列や $A_0 > A_1 > \cdots > A_\alpha > \cdots$ $(\alpha < \omega_2)$ なる列は $\mathfrak{P}$ のなかには存在しない．

2)
$$A_0 < A_1 < \cdots < A_\alpha < \cdots < \cdots < B_\beta < \cdots < B_1 < B_0$$
なる $\mathfrak{P}$ の上昇列 $\{A_\alpha\}_{\alpha<\omega_1}$ と $\mathfrak{P}$ の下降列 $\{B_\beta\}_{\beta<\omega_1}$ とが存在したとする．このとき $\mathfrak{P}$ の元 C で $\{A_\alpha\}_{\alpha<\omega_1} < C < \{B_\beta\}_{\beta<\omega_1}$
なるものが必ず存在する．

このような $\mathfrak{P}$ のことを **Hausdorff の超連続体** または単に超連続体と呼ぶことにする．

連続体が ω に対するものとするとき，超連続体が ω_1 に対するものであることは連続体のつぎの 2 つの性質を考えれば明らかであろう．

1) $A_0 < A_1 < \cdots < A_\alpha < \cdots$ $(\alpha < \omega_1)$ なる列や $A_0 > A_1 > \cdots > A_\alpha > \cdots$ $(\alpha < \omega_1)$ なる列は連続体のなかにはない．

2)
$$A_0 < A_1 < \cdots < A_n < \cdots < \cdots < B_m < \cdots < B_1 < B_0 \quad (n, m < \omega)$$
なる $\{A_n\}_{n<\omega}$，$\{B_m\}_{m<\omega}$ が連続体のなかにあったとき
$$\{A_n\}_{n<\omega} < C < \{B_m\}_{m<\omega}$$
なる点 C が連続体のなかにある．

2) は連続体の連続性の公理に相当するから，Hausdorff の公理の 2) をゲーデルはよく連続性の公理と呼ぶのである．

さて超連続体 $\mathfrak{P}$ の存在から，どんなことがでてくるのであろうか？ Hausdorff は Hausdorff の公理からつぎのことを証明した．

定理 3　連続体の濃度は $\aleph_1$ より大きい．さらにくわしくいえば $2^{\aleph_1} = 2^{\aleph_0}$ が成立する．

（証明）$2^{\aleph_1} \leqq 2^{\aleph_0}$ をいえば十分である．いま
$$2 = \{0, 1\}$$
と考えて
$$\Pi = \bigcup_{\alpha \leqq \omega_1} 2^\alpha$$

とおくことにする．すなわち $f\in\Pi$ なる f をとれば，f はある可付番順序数または ω_1 からその値が 0 か 1 である関数になっているわけである．いま Π の 2 元 f,g の間の関係 $\prec$ をつぎのように定義する．いま

$$f:\alpha\to 2$$

$$g:\beta\to 2$$

とする．つぎのようにいろいろの場合に分けて考える．

1）$\alpha<\beta$ で g が f の拡張になっているとき，すなわち

α より小さい順序数 γ については $f(\gamma)=g(\gamma)$

が成立しているとき，

このとき　　$f\prec g$ とは $g(\alpha)=1$

$g\prec f$ とは $g(\alpha)=0$

と定義する．

2）　$f(\gamma)\neq g(\gamma)$

であるような γ が存在するとき，このときはそういう

γ の最小のものを γ_0

として，

$f(\gamma_0)<g(\gamma_0)$ ならば $f\prec g$

$g(\gamma_0)<f(\gamma_0)$ ならば $g\prec f$

と定義する．この　$\prec$ が Π についての線型順序

になっていることは明らかであろう．

いま　　$\Pi_\alpha=\{f\in\Pi\mid f:\alpha\to 2\}$

と定義し，　　$\Pi_\alpha{}^0=\bigcup_{\beta<\alpha}\Pi_\beta$

と定義する．

いま，α が極限数であるとき Π_α の元 f に対して，$\Pi_\alpha{}^0$ の上昇列または下降列をとって f がその極限になるように考える．これを f をいろいろな場合に分けて定義する．

3.1）f が恒等的に 1 であるとき

この場合 $\beta<\alpha$ なる β に対して f_β を

$$f_\beta : \beta \to 2 \text{ で } \forall\gamma<\beta(f_\beta(\gamma)=1)$$

によって定義すれば

$$f_0 < f_1 < \cdots < f_\beta < \cdots \underset{(\beta<\alpha)}{\to} f$$

となる．

α が可付番順序数のときは

$$\alpha_0 < \alpha_1 < \cdots < \alpha_n < \cdots \underset{(n<\omega)}{\to} \alpha$$

なる $\alpha_0, \alpha_1, \cdots$ をとってきて　　$f_n' = f_{\alpha_n}$

と定義すれば

$$f_0' < f_1' < \cdots < f_n' < \cdots \underset{(n<\omega)}{\to} f$$

となる．このときは上昇列の極限になるが，下降列の極限にはならない．

3.2）f が恒等的に 0 であるとき

このときは 3.1）と同様に $\beta<\alpha$ なる β に対して f_β を

$$f_\beta : \beta \to 2 \text{ で } \forall\gamma<\beta(f_\beta(\gamma)=0)$$

とすればよい．α が可付番ならば，3.1）の場合と同じように $f_0', f_1', \cdots$ を定義する．このときは下降列の極限になるが，上昇列の極限にはならない．

3.3）f の値のなかに 0 も 1 もあるが十分先はすべて 1 になってしまうとき

このとき f が最後に 0 をとる値を α_0 とする．すなわち

$$f(\alpha_0)=0 \text{ で } \alpha_0 \text{ のあとはすべて } 1$$

をとるものとする．このとき $\beta<\alpha$ なる β に対して

$$f_\beta : \beta \to 2$$

を

$$\forall\gamma<\beta(f_\beta(\gamma)=f(\gamma))$$

によって定義すれば，明らかに

$$f_{\alpha_0} < f_{\alpha_0+1} < \cdots < f_\beta < \cdots \underset{(\alpha_0 \leq \beta \quad \alpha)}{\to} f$$

となる．

α が可付番のときは 3.1）と同様に $f_0', f_1', \cdots$ を定義する．またさらに $\alpha_0<\beta<\alpha$ に対して

$$g_\beta : \beta \to 2$$

なる g_β に

$$\forall\gamma<\alpha_0(g_\beta(\gamma)=f(\gamma))\wedge g_\beta(\alpha_0)=1\wedge\forall\gamma(\alpha_0<\gamma<\beta \to g_\beta(\gamma)=0)$$

と定義すれば　$g_{\alpha_0+1}>g_{\alpha_0+2}>\cdots>g_\beta>\cdots \underset{(\alpha_0<\beta<\alpha)}{\to} f$

となる．α が可付番のときはやはり部分列 $g_0', g_1', \cdots, g_n' \cdots$ $(n<\omega)$ をとることにする．

3.4）f の値のなかに 0 も 1 もあるが十分先はすべて 0 になってしまうとき　3.3）のときと同様に定義する．

3.5）上のいずれの場合でもないとき

まず　$\alpha=\omega_1$

の場合を考えよう．このとき f が 1 をとる値を全部並べて

$$\mu_0<\mu_1<\cdots<\mu_\beta<\cdots \qquad (\beta<\omega_1)$$

とし，f が 0 をとる値を全部並べて

$$\nu_0<\nu_1<\cdots<\nu_\beta<\cdots \qquad (\beta<\omega_1)$$

とする．

$$f_\beta : \mu_\beta \to 2 \text{ を } \forall\gamma<\mu_\beta(f_\beta(\gamma)=f(\gamma))$$

によって定義すれば，明らかに

$$f_0<f_1<\cdots<f_\beta<\cdots \underset{(\beta<\omega_1)}{\to} f$$

となり，また　$g_\beta : \nu_\beta \to 2$　を　$\forall\gamma<\nu_\beta(g_\beta(\gamma)=f(\gamma))$

によって定義すれば，明らかに

$$g_0>g_1>\cdots>g_\beta>\cdots \underset{(\beta<\omega_1)}{\to} f$$

となる．

つぎに α が可付番順序数のときを考える．このとき f が 1 をとるような $\mu_0<\mu_1<\cdots<\mu_n<\underset{(n<\omega)}{\cdots\to}\alpha$ なる $\mu_0, \mu_1, \mu_2, \cdots$ と，f が 0 をとるような $\nu_0<\nu_1<\cdots<\nu_n<\underset{(n<\omega)}{\cdots\to}\alpha$ とをとることができる．この μ と ν とについて上と同じようにすればよい．

さて定理の証明は Π から $\mathfrak{P}$ へ 1 対 1 の大小の順序を保つ写像 H を

定義していけばよい．これを Π_α について α についての超限帰納法で定義していくのである．最初に $\mathfrak{P}$ から相異なる 2 点 A, B をとってきて $A<B$ であるとする．いま $\alpha<\omega_1$ であるときは，Π_α の元の H による値はすべて A と B との間に入っているものとする．超限帰納法によって順々に定義していくのであるから $\Pi_\alpha{}^0$ の元に対しては H がすでに大小の順序を保つように定義されているものとする．(すなわち $f<g \to H(f)<H(g)$)．いま H を $\Pi_\alpha{}^0 \cup \Pi_\alpha$ の上に拡張して，やはり大小の順序を保ち A と B との間にあるようにすればよい．これをするためにまず最初に α を可付番として，$f \in \Pi_\alpha$ とするとき，α についての超限帰納法によって，つぎのことが容易に証明できる．(α が極限数の場合，極限数でない場合，ない場合はさらに $\alpha-1$ が極限の場合，そうでない場合と場合を分ければ簡単である．)

＊）f が Π_α の最大元でも最小元でもなければ，$\Pi_\alpha{}^0$ の高々可付番な部分集合 F と G とで，$F<f<G$ で F と G との間にある Π_α の元は f だけであるようなものがある．

さて H の定義をすることにする．まず α が可付番であるとして $f \in \Pi_\alpha$ をとってくれば

f が Π_α の最大元でも最小元でもない

ならば ＊）によって $\Pi_\alpha{}^0$ の高々可付番部分集合 F, G で

$$F<f<G$$

で F と G の間の Π_α の元は f だけなものがある．

$$\mathfrak{S}=\{H(h)\,|\,h \in F\},$$

$$\mathfrak{T}=\{H(h)\,|\,h \in G\}$$

と定義すれば，帰納法の仮定により

$$\mathfrak{S}<\mathfrak{T}.$$

また $\mathfrak{S}$ も $\mathfrak{T}$ も高々可付番であるから，

$$\mathfrak{S}<C<\mathfrak{T}$$

なる $\mathfrak{P}$ の元 C が存在する．このような C の 1 つを $H(f)$ と定義すればよい．

もし　　　　　　　　　　f が Π_α の最大元

ならば，$\Pi_\alpha{}^0$ の元　　　$f_0 < f_1 < \cdots < f_n \underset{(n<\omega)}{<\cdots} \to f$

なる $f_0, f_1, \cdots$ をとってきて，

$$\mathfrak{S} = \{H(f_n) \mid n < \omega\},$$

$$\mathfrak{T} = \{B\}$$

として同様のことをすればよい．f が Π_α の最小元であるときも同様である．

つぎに $\alpha = \omega_1$ のときを考えて，$f: \omega_1 \to 2$ とする．もし

f が Π_{ω_1} の最大元ならば $H(f) = B$

と定義し，もし　f が Π_{ω_1} の最小元ならば $H(f) = A$

と定義することにする．したがっていま

f は最大元でも最小元でもない

ものとする．このとき $\Pi_{\omega_1}{}^0$ の元 $f_0, \cdots, f_\beta, \cdots, g_0, \cdots, g_\beta, \cdots$ $(\beta < \omega_1)$ をとってきて

$$f_0 < \cdots < f_\beta \underset{(\beta<\omega_1)}{<\cdots} \to f$$

$$g_0 > \cdots > g_\beta \underset{(\beta<\omega_1)}{>\cdots} \to f$$

が成立するようにできる．帰納法の仮定により

$$H(f_0) < \cdots < H(f_\beta) \underset{(\beta<\omega_1)}{<\cdots} \underset{(\beta<\omega_1)}{<\cdots<} H(g_\beta) < \cdots < H(g_0)$$

が成立する． Hausdorff の連続性の公理により

$$H(f_0) < \cdots < H(f_\beta) \underset{(\beta<\omega_1)}{<\cdots<} C \underset{(\beta<\omega_1)}{<\cdots<} H(g_\beta) < \cdots < H(g_0)$$

なる C が $\mathfrak{P}$ に存在する．このような

C の 1 つを $H(f)$

と定義すればよい．

いままで Hausdorff がしたところまでのべた．いよいよゲーデルの考えたところをのべることにする．その前にちょっと断っておきたいのは，じつは Hausdorff はいろいろなことを雑然と考えたのであって，それに方向をあたえて，こういうふうに考えることが大切であるというふうにとりだしとりあげたのはゲーデルである．したがっていままでにのべたことは Hausdorff が

やったことにはちがいないが，その全体の考え方にはゲーデルの思想やアイディアが入っているといっても過言ではない．

つぎにいままでに Hausdorff の公理についてのべたが，Hausdorff はもちろん公理としてとりあげたわけではないし，ほんとうらしいともいっていない．どうしてこれがほんとうらしいか？ ということになると私自身漠然と気分がわかる程度で全然自信がない．ただゲーデルはこの事柄についてはかなり長い期間熟考したようであり，私などにはない独特の直観を超連続体に対してもっているようである．数学的対象に対するわれわれの直観は，長い間その事柄について考え，模索したうえではじめてできるものであるから(100年前にどの数学者が現代数学者のもっているような直観を集合に対してもっていたであろうか！）　私自身ゲーデルに近いくらいこのことについて考えてみたうえでなければ，ゲーデルの考えについての自分なりの意見をのべることすらできない．ただ，いままでのゲーデルの業績からいって，十分な理由がなければ公理としては提出しないだろう，と彼のことを信頼するだけである．その意味でこの事柄に対する研究がどんどん進んで早くわれわれにもよい直観ができてこの事柄について判断ができるようになる時期がくることを待ち望んでやまない．

新しい公理

さてゲーデルの公理をのべるために ω_n から ω_n への関数の間にも $<$ という関係を定義することにする．いま f と g とがともに

$$f: \omega_n \to \omega_n,\quad g: \omega_n \to \omega_n$$

なる関数であるとする．このとき

$$f < g$$

を

$$\exists \alpha < \omega_n \forall \beta (\alpha < \beta < \omega_n \to f(\beta) < g(\beta))$$

によって定義する．

いまこのほかに

$$f \leqslant g$$

なる関係を

$$\forall \alpha < \omega_n (f(\alpha) < g(\alpha))$$

によって定義することにする．

さてゲーデルの公理は Hausdorff の公理につぎの公理をつけ加えたものである．

〈ゲーデルの公理〉

$\omega_n^{\omega_n}$(ω_n から ω_n への関数全体の集合）の部分集合 F と M とでつぎの条件をみたすものがある．

1）F は $<$ で整列されており，その順序型は ω_{n+1} である．

2）$\forall f \in \omega_n^{\omega_n}\ \exists g \in F(f<g)$

3）M の濃度は $\aleph_{n+1}$ である．

4）$\forall f \in \omega_n^{\omega_n}\ \exists g \in M(f \leqslant g)$

5）$\{f\lceil\alpha \mid \alpha<\omega_n \wedge f \in F\}$ の濃度は $\aleph_n$ である．

ここに $f\lceil\alpha$ は f を α までに制限してできる関数のことである．すなわち

$$g:\alpha \to \omega_n \quad \text{で} \quad \forall\beta<\alpha(g(\beta)=f(\beta))$$

をみたす関数 g のことである．

6）$\{f\lceil\alpha \mid \alpha<\omega_n \wedge f \in M\}$ の濃度は $\aleph_n$ である．

以上がゲーデルの公理である．この場合もなぜこれが公理として提出されるだけの理由があるのか私にはわからないが，ともかくまず研究してその後でよく熟考してみたいものである．

ゲーデルは，Hausdorff の公理とゲーデルの公理から連続体の濃度が $\aleph_2$ であることがでてくるといっているのであるが，その証明は大きいペン字でたった 5 枚の紙に書いてあるだけである．私の学生の一人がいま暗号解読にあたっているが，まだ解読に成功していない．ゲーデルから訂正版が送られてくるのと，学生の暗号解読とどちらが早いか？　ちょっと興味のあるところである．

暗号解読はまだできていないし，ゲーデルは間違いがあるということであるし，ゲーデルの証明にはここではふれない．

しかしながら，その証明の中心らしいところをながめているとゲーデルは超連続体の存在を用いて，より深い解析学を作ろうとしたのではないか？

と思われるふしがある．いやこういってはいいすぎになるのであって，私がそういう可能性があるのではないか？ と思ってやってみたくなるといったほうが正確かもしれない．とにかく超連続体の濃度を離れても極度に興味があることのように思われるし，いずれにしてもこのところが証明の1つの中心であると思うのでこのことについて私が現在思っていることを少しばかり説明してみたいと思う．

超連続体で超解析学

いま $\mathfrak{P}$ を超連続体とする．いま $\mathfrak{P}$ には恒等的に 0 の点列すなわち (0, 0, 0, …) が入っているものと思ってもよい．（もしそうでなければ，$\mathfrak{P}$ の 1 つの点列 $a_0, a_1, \cdots$ をとりだして $\mathfrak{P}'=\{(b_0-a_0, b_1-a_1, \cdots) \mid (b_0, b_1, \cdots)\in\mathfrak{P}\}$ を考えればよい．）これを O と書くことにしよう．

ゲーデルのやっていることは，Lebesgue 測度よりもう少し精密な測度をあたえようということである．

Lebesgue 測度は非常に有効な測度であるが，測度 0 という集合の族が，ほとんど実数のすべての族と同じくらいたくさんの集合を含んでいる族である．その点でいえば，きわめて粗雑な測度である．ここでやろうとするのは Lebesgue 測度 0 のものをさらに細かく分類するような測度を作ろうということである．もちろんその値が実数では不可能である．ゆえにその値を実数ではなくて超連続体の元をとってくることによってもっと精密な測度を作るのである．

ところでこの新測度の定義があまりハッキリしないのである．ゲーデルにしてみれば何年も考えた挙句であたりまえと思ったことを書いてあるのだろうが，第三者にはアイマイでいろいろな可能性があるので全然わからない．もうちょっとキチンと書いておいてくれれば助かるのにと思うのだが，こんなことをいってもはじまらない．ここでは 2 つの候補をあげてそれについて考えることにする．とにかくいま Lebesgue 測度 0 の集合 Z があたえられているものとする．面倒であるからいま $Z\subseteq[0,1]$ を仮定する．

第一候補

$\mathfrak{P}$ の点 $A=(a_1, a_2, \cdots)$ が

$$\mu(Z)\leqslant A$$

であるというのは，十分大きい n_0 をとるとき，$n\geq n_0$ なる n について，n 個の開区間 $I_1, \cdots, I_n$ をとってきて

可付番個の点をのぞいて $I_1\cup\cdots\cup I_n$ が Z をおおい

そのうえ　$$l(I_1)+\cdots+l(I_n)=a_n$$

にできることである．ここに $l(I)$ というのは‘I の長さ’のことであって，$I=(a,b)$ ならば $l(I)=b-a$ と定義する．

$I_1\cup\cdots\cup I_n$ が可付番個の点をのぞいて Z をおおうというのは，可付番な集合 A が存在して

$$Z\subseteq A\cup I_1\cup\cdots\cup I_n$$

となることである．ここでは開区間を用いたが可付番個の点をのぞいて考えているのであるから，閉区間を用いても同じことである．

さて，この新しい測度がどれくらい有効か考えてみることにしよう．有効さの1つのメヤスは新しい測度で O であるような集合がどんな集合になるか？ということであろう．新しい測度で O な集合がたしかに小さいものであればこの測度は少なくとも十分細かい分類をあたえるものといってよいだろう．これを調べるために少しばかり定義をすることにする．

定義　点 x が Z の $\aleph_1$ 点であるというのは，x のいかなる近傍 U をとってきても，

$$\overline{\overline{U\cap Z}}\geqslant\aleph_1$$

であることと定義する．

定理 4　Z の $\aleph_1$ 点の全体を F とすれば，F は空集合であるか，または閉な完全集合である．

(証明)　$\aleph_1$ 点でない点 x には，x の近傍 U をとって，U のすべての点が $\aleph_1$ 点でないようにできるから，$\aleph_1$ 点でない点の全体は開集合である．

ゆえに　　F は閉集合

であることがわかった．ゆえに F が孤立点をもたないことをいえばよい．

いまもし　　F の点 x が孤立点

であったとすれば，x の近傍 U をとって

$$U\cap F=\{x\}$$

であるようにできる．$U-\{x\}$ のすべての点 y について，十分小さい y の近傍 V をとれば　　$\overline{\overline{V\cap Z}}\leqslant\omega$

であるようにできる．いま実数の空間は第 2 可付番公理をみたすから，$U-\{x\}$ はこのような V の可付番個の和集合になっているといってよい．

ゆえに　　$\overline{\overline{(U-\{x\})\cap Z}}\leqslant\omega$

がでる．したがって　　$\overline{\overline{U\cap Z}}\leqslant\omega$

となって x が $\aleph_1$ 点である仮定に反する．

定理 5　$I_1,\cdots,I_n$ を $[0,1]$ に含まれた閉区間とする．いま F を Z の $\aleph_1$ 点の全体の集合とするとき，Z が可付番個の点をのぞいて $I_1\cup\cdots\cup I_n$ でおおわれることと $F\subseteq I_1\cup\cdots\cup I_n$ とは同値である．

（証明）　定理 4 の証明と同じことをくり返すことによって，

$Z-F$ が高々可付番

であることがわかる．ゆえにもし

$$F\subseteq I_1\cup\cdots\cup I_n$$

であれば，　Z が可付番個の点をのぞいて $I_1\cup\cdots\cup I_n$ でおおわれることは明らかである．

いま逆に Z が可付番個の点をのぞいて $I_1\cup\cdots\cup I_n$ でおおわれているとしよう．　　$x\notin I_1\cup\cdots\cup I_n$

なる x をとると，　$Z-(I_1\cup\cdots\cup I_n)$ は高々可付番

であってこれは開集合であるから x は $\aleph_1$ 点ではない．すなわち

$$x\notin F$$

となる．ゆえに　　$F\subseteq I_1\cup\cdots\cup I_n$

がいえた．

定理 6　もし Z が非可付番とすれば，すべての自然数 n について，l_n を Z が可付番個の点をのぞいて $I_1 \cup \cdots \cup I_n$ に含まれるような $l(I_1)+\cdots+l(I_n)$ の下限と定義すれば

a）　$l_n > 0$ であり，

b）　Z を可付番個の点をのぞいておおう $I_1 \cup \cdots \cup I_n$ で $l(I_1)+\cdots+l(I_n) = l_n$ なる $I_1, \cdots, I_n$ が存在する．

（証明）　[0,1] 区間には端の点 0 と 1 とがあるのでじつは整然と証明することがやっかいである．ここでは概略のみをのべることにする．まず Z の $\aleph_1$ 点の全体を F とおいて

$$(0,1)-F$$

を考えてみよう．これは開集合であるから，開区間 $J_1, J_2, J_3, \cdots$ で

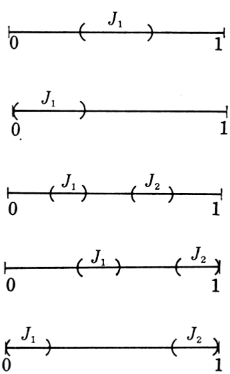
c）　$(0,1)-F = J_1 \cup J_2 \cup J_3 \cup \cdots$

d）　$J_i \cup J_j = \phi \qquad (i \neq j)$

e）　$l(J_1) \geq l(J_2) \geq l(J_3) \geq \cdots$

なるものが存在する．ここで e）は $J_1, J_2, J_3, \cdots$ を長さの大きさの順に並べれば，$l(J_1)+l(J_2)+\cdots \leq 1$ から自然にでてくることである．

このことは，(0,1) から Z の $\aleph_1$ 点を 1 個も含まないような開区間で一番大きいものを 1 つとる方法は J_1 をとることであることを意味しており，



残りが 2 個

残りが 1 個

残りが 3 個

残りが 2 個

残りが 1 個

一番大きい 2 個の閉区間をとることは $J_1 \cup J_2$ をとること …… を意味している．何個閉区間をとるということと，残った部分が何個の閉区間になっているか？ ということは前ページの図でみるように異なった問題である．

またそのうえ $l(J_1)=l(J_2)=\cdots=l(J_k)$ ということがありえ，そのうち何個かが端にまでおよんでいる場合がありえてキチンと分類するのは面倒臭いが，とにかく端の点は 2 個しかなくちょうど n 個の閉区間で残りがおおわれる可能性は最初の $J_1,\cdots,J_n,\cdots,J_{n+k}$ で $l(J_{n+2})=l(J_{n+3})=\cdots=l(J_{n+k})$ が成立する一番大きい $n+k$ のところまでとって（この k は必ず有限回でつきてしまう．なぜならば $l(J_i)>0$ で $l(J_1)+\cdots+l(J_i)+\cdots<1$ であるからである．）この $J_1,\cdots,J_{n+k}$ のうちどれだけをとったものがちょうど n 個の閉区間 $I_1,\cdots,I_n$ でおおわれていてその $l(I_1)+\cdots+l(I_n)$ が最小の値になっているかを有限回の場合にあたって調べてみればよい．この最小の $I_1,\cdots,I_n$ をとってくると

$$l_n=l(I_1)+\cdots+l(I_n)>0$$

であることは明らかであろう．

定理 7　$\mu(Z)=O$ ならば，Z は高々可付番である．

（証明）　Z が非可付番とすると，Z の $\aleph_1$ 点の集合 F は空でない．ゆえに定理 6 の $l_1,l_2,l_3,\cdots$ を作れば

$$l_n>0$$

である．いま

$$L=(l_1,l_2,l_3,\cdots)$$

とおこう．いまさらに超連続体 $\mathfrak{P}$ の O より大きい任意の点 $A=(a_1,a_2,\cdots)$ をとってくると

$$\mu(Z)=O<A$$

から，十分大きい a_n をとれば　$l_n\leq a_n$

が成立する．ゆえに

$$O<\left(\frac{l_1}{2},\ \frac{l_2}{2},\ \frac{l_3}{2},\cdots\right)<A$$

がすべての O より大きい $\mathfrak{P}$ の元 A に対して成立する．これは $\mathfrak{P}$ が極大であるという仮定に反する．

さて定理 7 はわれわれの測度 μ がきわめて細かい測度であることを示し

ていて，われわれの測度が将来性十分であるように思われる．しかし問題をもとにもどしてこれがゲーデルの意中の測度であるか？ と考えてみるときわめて疑わしい．じつは一番はじめに断るべきであったが，第一候補という意味は一番よい候補という意味ではなくて，学生が何を考えてよいかわからなくて面クラッテいるので，私がまあ臨時にこう定義して考えてみたらどうか？ といって最初にもちだしたからという，ただそれだけの理由で第一候補なのである．

どうもゲーデルの考えている測度ではないらしいという根拠は，ゲーデルの測度はどうもつぎの条件をみたしているように思えるからである．

ある $[0,1]$ の増加部分集合列 $A_0 \subseteq A_1 \subseteq \cdots \subseteq A_i \subseteq \cdots$ $(i<\omega_1)$ が存在して

$$\mu(A_0)<\mu(A_1)<\cdots<\mu(A_i)<\cdots$$

となる．

ところでわれわれの測度は絶対にこの性質をみたさないのである．このことを証明しよう．

補題　いま　$A \subseteq B \subseteq [0,1]$ で $\mu(A)<\mu(B)$

とすれば，無限に多くの n について

$$l_n(A)<l_n(B)$$

であり，またすべての n について

$$l_n(A) \leq l_n(B)$$

である．ここに l_n は定理 6 で定義されたものである．

(証明)　$$l_n(A) \leq l_n(B)$$

は $A \subseteq B$ から明らかである．いま

$l_n(A)<l_n(B)$ なる n が有限個しかない

とすれば，　その有限個をのぞいては $l_n(A)=l_n(B)$

したがって $\mu(A)$ と $\mu(B)$ との間には $\mathfrak{P}$ の元はありえなく，

矛盾する．

定理 8　$A_0 \subseteq A_1 \subseteq \cdots \subseteq A_i \subseteq \cdots_{(i<\omega_1)} \subseteq [0,1]$ で $\mu(A_0)<\mu(A_1)<\cdots<\mu(A_i)<\cdots$ であることはありえない．

(証明)　任意の

$$i<\omega_1$$

なる i をとって考えよう．補題により

$$l_n(A_i)<l_n(A_{i+1})$$

なる n が存在する．ところで

$$i \text{ の全体は } \omega_1 \text{ 個,}$$

$$n \text{ の全体は } \omega \text{ 個}$$

であるから，ある n_0 に関しては非可付番個の $i_0<i_1<\cdots<i_\alpha<\cdots$ $(\alpha<\omega_1)$ が存在して

$$\alpha<\beta \to l_{n_0}(A_{i_\alpha})<l_{n_0}(A_{i_\beta})$$

が成立することになる．ところで実数の長さが ω_1 であるような狭義単調増加列は存在しない（竹内『現代集合論入門』日本評論社，221 ページ）からこれは不可能である．

超連続体 $\mathfrak{P}$ について，われわれは直観なしに議論をするのでどうしても話が抽象的になってしまう．ここにちょっとした演習問題をあげておく．

演習問題　Z をカントールの集合（カントールの不連続体，または 3 進集合）とするとき，$l_1, l_2, l_3, \cdots$ がどうなるかを計算せよ．

第二候補

第一候補はそれ自身としての興味があるが，どうやらゲーデルの考えているものではないらしい．となるとゲーデルの考えているものはどんなものであろうか？　いまのところはわれわれには推量以外にない．しかし小生の学生はつぎのものがそうではないか？といま考えている．

いま $A=(a_0, a_1, a_2, \cdots)$ をとったとき

$$\nu(Z)\leqq A$$

をつぎの条件をみたす開区間 $I_0, I_1, I_2, \cdots$ が存在することと定義する．

1)　すべての $i<\omega$ について，Z は $\aleph_1$ 個の点をのぞいて $I_i\cup I_{i+1}\cup\cdots$ でおおわれている．

2)　十分大きい n についてはいつでも

$$l(I_n) \leq a_n$$

が成立している．

超連続体 $\mathfrak{P}$ については $\nu(Z) \leqslant A$ なる $\mathfrak{P}$ の点 A の全体が定めるデデキント流の切断によって $\mathfrak{P}$ の上の $\nu(Z)$ の値を決めるのである．

小生もこの測度の方がゲーデルの考えているものに近いであろうと学生の意見に賛成なのであるが，この測度の難点はむずかしすぎていろいろの性質がなかなかわからないというところにある．（したがって，ゲーデルのに近いであろうというわれわれの推量はあて推量以上のものではなくなる．）この間の事情はつぎの簡単な演習問題をキチンと証明してみれば，よくわかることと思う．

演習問題　Z をカントールの集合とするとき

$$\nu(Z) \leqslant \left(\frac{1}{10}, \frac{1}{100}, \frac{1}{1000}, \cdots\right)$$

は成立しない．

まだ細かいことや，いろいろな実例についてのべたくもあるがまた反面において，ゲーデルが間違っていて，直すといっており，われわれの暗号解読が未だ十分に進んでいないものについてあまり細かいところまで議論するのもどうか？と思われる．

しかし，ゲーデルの直観が何か？　ゲーデルの証明はじつはどんなものか？（具体的にはゲーデルの訂正は公理の訂正も含むのか？）等についての好奇心ばかりではなく，もしこういう考えが妥当ならば超連続体というものが意外に数学のなかで活躍する可能性もあるのではないか？という私の独走しすぎたキライのある考えにひかれて，一応紹介してみたかったのである．

案外この原稿がでるころにはもっとくわしいことがわかっているかもしれない．そういう場合でも，暗号解読に成功した場合でも，できれば結果の報告だけはしたいと思っている．なお私は Hausdorff の Pantachie という術語が面白くて用いたが，英語では complete scale というのが普通であり，ゲーデルも complete scale を用いている．

学会での反応

じつはここまで書いてから私はカナダとアメリカの 2 つの学会に出席した．そこでこの方面の専門家といわれる人達といろいろとゲーデルのこの新しい考えについての information を交換した．驚いたことにほとんどの人がこのことについては何も知らなかった．まずプリンストンにいる Dana Scott に会った．彼はまだ読んでいないようで数学的なことについてはウワサ以上は何も知らなかったが，なぜゲーデルがあのようなカキナグリの原稿をタルスキーに送ったかということについての彼の意見を伝えてくれた．1970 年の春ごろゲーデルは極端に身体の調子が悪く彼自身は死期が近づいたと思ったらしい．彼はこのまま死んでしまうと，彼が長い間考えた，この重大な考えがそのまま誰にも知られずに消えてなくなってしまうことを恐れて，病のうちに書いたとのことである．その後ゲーデルは健康を回復して昔ながらの彼にもどったのである．（それもそれほど健康というわけではないが.）

この話をのぞいて新しい情報というものは何もなかった．第一に読んだといわれている人が，皆の意見では，Solovay, Martin, Shoenfield と 3 人しかいず，そのうち Shoenfield しか学会にきていなかった．彼は Martin と一緒に読んだが，どうしても筋道が通らないからやめたといって，それもだいぶ前のことだからということで私がもう少しくわしいところでディスカッションをしようと思ったができなかった．

読んでいる人はいなくても噂話だけは盛んであった．しかしほとんどが冷いものであった．1 番目のえらい set theorist（カントールのことだろう）が連続体の濃度は $\aleph_1$ だといったから，こんどは 2 番目のえらい set theorist が連続体の濃度は $\aleph_2$ だというのだろう，というのとか，you know, he is mentally ill というひどいのまであった．しかしその一番ヒドイことをいった人は用心深くつけ加えた，“あと 20 年ほどたって誰かがうんといい仕事をすると，これがゲーデルのいっていたことだということになるだろう.”

A. Robinson はゲーデルの公理についてのコミッティーを作って，いろいろの断片をつなぎ合わせてどんなことか想像したらよいと冗談まじりにいっていた．Moschovakis は C.C.Chang がゲーデルからタルスキーへの原稿の first Xerox copy をもっていると得意がっていると笑っていた．（ゼロックス・コピーに最初も 2 番目もないだろうが，いままで読んだ人のほとんどがタルスキーから直接ではなくて Chang のコピーのコピーであるから，Chang が得意がるのもマンザラ意味のないことではない.）

ただ Tennenbaum 一人がこれは将来の集合論をユリウゴカス大事件になるといっていた．もっとも彼は集合論のなかでの無矛盾性や独立性をやっている人達に，お前達の仕事はそうなったら意味がなくなるぞと厭味をちょっというらしい．(私が Tennenbaum に会ったのは彼の家で，彼自身はいま身をひそめて学会にでてこないのでこれは彼が人にいっているといったことで私が実際に目撃したわけではない.）

ほんとうに将来この事件がどのような発展をとげるかは興味津々である．

一つ念のためにつけ加えておくが，超連続体とか，超連続体によって超解析学を！というようなことはすべて私が勝手につけ加えたことでゲーデル自身がいっていることではない．ゲーデル自身がいっているのは，あくまでも連続体の濃度が $\aleph_2$ であるということが，彼の信ずる公理からでてくるということだけである．先ほどの Moschovakis にいわせれば，もしゲーデルが簡単に“連続体の濃度は $\aleph_2$ である”と公式声明をすれば自分は信ずるのだが，理由をつけられるとかえってわからなくなる，といっていた．

私にとっては，すべてはゲーデルがかけたくらいの時間をかけて，彼のいっていることがよくわかるようになるまで表面的な判断は避けるべきであるように思われる．

体の理論とロジック

I　実閉体の決定問題

この頃はロジックが数学の各分野にだんだん用いられるようになってきて，大変喜ばしいことである．整数論でアメリカ数学会の賞をもらった Ax-Kochen の仕事，それにハルモスの予想を解いた A. Robinson の仕事というふうに各々の分野でロジックが本質的に用いられるようになってきた．この調子でいけば将来にはロジックというのは数学の各分野の常識的な常用の手段ということになるだろう．私は専門がロジックの応用ではないが，これは私にとってもなかなか心強いことにはちがいない．

ところでロジックの定理で数学に最初に実用に用いだされた定理といえば何であろうか？　もちろん完全性定理というような最も基本的な定理をもちだしておけばまったく安全な答であるが，もう少し細かい定理というと何であろうか？　私にはタルスキーの実閉体についての決定問題がそうであるように思われる．私はもう 10 年以上も前にヘルマンダーが微分方程式にこれを応用しているのを見てビックリしたものである．

ここでは，代数学とロジックをホンのチョッピリ知っている人のためにこのタルスキーの結果を証明することにする．

1.　体の言語

ここで，まず体についてのべるのであるが，まずロジックらしく体についてキチンとのべることにする．まずロジックでは体の定義をするのに必要な言葉について考える．そしてそれを体の**言語**（language）というのである．

体の言語はつぎのものから構成される．

特別な体の元を表わす記号　　$0, 1$

変数　　$a, b, c, \cdots, x, y, z$

体の元に関する演算を表わす特別な関数記号

$$\cdot,\ +,\ -,\ ^{-1},$$

等号　　$=$

論理記号　　$\neg, \wedge, \vee, \rightarrow, \leftrightarrow, \forall, \exists$

以上が体の言語を構成するものの全体である．

以下ロジックの正式な手続きにしたがって，体の言語についていろいろな概念を構成していくことにする．まず第一に **term**（**項**）について定義をする．これは $a+b$ というように記号が組み合わされた形（このなかに $a, b, 0, 1$ のような 1 つの文字だけのものも含めることにする）であって実際には体の元を表わすものである．

体の言語の term はつぎのごとく定義される．

1)　$0, 1$ および任意の変数は term である．

2)　s と t とが term であるとき，$(-s)$，(s^{-1})，$(s+t)$ および $(s\cdot t)$ は term である．

3)　以上によってできたもののみが term である．

以上によってたとえば

$$(((a+b)\cdot(c^{-1}))+(-1))$$

が term であることが容易にわかる．もっとも条文としては以上のように厳密な定義をするが，実際には普通のように簡単に

$$(a+b)\cdot c^{-1}-1$$

と書く．ほんとうはカッコの省略法についてキチンとしたルールをのべるべ

きであるが，一応広くゆきわたっているので慣用の流儀にしたがうことによってそれを正確に表現することを省略するわけである．そのうえさらに慣用にしたがって，上の term は

$$\frac{a+b}{c}-1$$

というふうに書くことにする．

さらに普通のように $x\cdot x$ を x^2, $x\cdot x\cdot x$ を $x^3,\cdots$ という省略記号を用いる．したがって

$$\frac{a_0x^n+a_1x^{n-1}+\cdots+a_n}{b_0y^m+b_1y^{m-1}+\cdots+b_m}$$

というような形はすべて体の term になるわけである．ここでもちろん n とか m とかは $0,1,2,\cdots$ というふうにハッキリ決まったあたえられた自然数でなければならない．したがって上に $\cdots$ と書いてあるところは実際にはすべて書きつくされているものでなければならない．ここでもう少しくわしくいうと $a_1+a_2+a_3+a_4$ というような形は普通と同じく，たとえば（ほんとうはドンナふうにカッコをつけ加えても構わないが）

$$(((a_1+a_2)+a_3)+a_4)$$

というふうにカッコをつけ加えたものの省略記号だと思うのである．

さて同様な方法で，体の言語の **formula** について定義しよう．

formula はつぎのように定義される．

1) s と t とが term であるとき，$s=t$ は formula である．この場合とくに atomic formula と呼ぶことにする．

2) A と B とが formula のとき，$(\neg A)$, $(A\wedge B)$, $(A\vee B)$, $(A\rightarrow B)$ および $(A\leftrightarrow B)$ も formula である．

3) A が formula であるとき，$(\forall xA)$ の形や $(\exists xA)$ の形も formula である．

4) 以上によってできたもののみが formula である．

ここでもわれわれは常識にしたがってカッコを省略するのである．たとえばたいてい一番外側のカッコは省略するのが普通であり，また $\neg A\wedge B$ と

書いたときは $((\neg A)\wedge B)$ の略であり，$A\vee B\rightarrow C\wedge D$ と書いたときは $((A\vee B)\rightarrow(C\wedge D))$ の略であると思うのである．一般に $\neg$ が結合力が一番強く，つぎに $\wedge$ と $\vee$ で $\rightarrow$ と $\leftrightarrow$ が一番弱いと考えるのである．$\forall$ や $\exists$ については誤解が生じ易いのでなるべくカッコを省かないのが普通である．上に結合力ウンヌンということの説明をしなかったが上にあげた例から判断していただきたい．もちろんここにつけ加える必要はないと思うが

$\neg A$ は ‘A でない’

$A\wedge B$ は ‘A であってかつ B’

$A\vee B$ は ‘A であるかまたは B’

$A\rightarrow B$ は ‘A ならば B’

$A\leftrightarrow B$ は ‘A と B とは同等である’

$\forall xA$ は ‘すべての x について A が成立する’

$\exists xA$ は ‘ある x が存在して A をみたす’

というふうに読むのである．たとえば

$$\exists x(ax^2+bx+c=0)$$

というのは 2 次式 ax^2+bx+c の根が存在することを意味している．

さらに $\forall xA$ か $\exists xA$ において，この A のなかの x はここで**束縛される**という．いま 1 つの formula のなかのある場所における変数 a は，1 度も束縛されることがなければ，**自由変数**である，という．ロジックにいろいろな流儀があってはじめから自由変数だけ用いる変数と，束縛される変数にだけ用いる変数というふうに分けてやる方法もあってじつは私はそのほうが好きなのであるが，実際にたくさんの式を書くときは変数が足りなくなって困るので，ここではその流儀はとらないことにする．

1 つも自由変数を含まない formula のことを，**命題**と呼ぶことにする．たとえば

$$\forall a\forall b\forall c\exists x(ax^2+bx+c=0)$$

というのは命題である．しばしばこのような $\forall a\forall b\forall c$ というような形は $\forall a, b, c$ というふうに略する．すなわち

$$\forall a, b, c\ \exists x(ax^2+bx+c=0)$$

というふうに書くのである．存在記号のほうも同様で $\exists x \exists y$ のことを $\exists x, y$ というふうに書くことが多いのである．以下においてわれわれは混乱の恐れがないかぎり formula と命題とをあまり区別せずにゴッチャに用いることとする．

万一
$$\exists x(ax^2+bx+c=0)$$
というような formula が命題として用いられていたらいつでも必要なだけ $\forall$ を前につけ加えて命題に直して考えてほしい．すなわちこの場合は

$$\forall a \forall b \forall c \exists x(ax^2+bx+c=0)$$

とするわけである．すなわち formula の先頭にある $\forall$ はしばしば省略することにする．$\exists$ は絶対に省略しない．

2. 体の公理

さてわれわれは体の言語について一通りのべたので，ここで体の公理を全部書き下すことはなんでもない．しかしこれはかなり紙数のムダであるように思うので，体の公理については代数学の本を見て，それをいまのわれわれの言語のなかに正確に書き下すことは演習問題としておきたい．

2, 3 体の公理の例をあげることにすれば

$$\forall x \forall y(x+y=y+x)$$

$$\forall x \forall y \forall z(x\cdot(y+z)=x\cdot y+x\cdot z)$$

さらにこれを $x+y=y+x$ と省略する習慣にしたがって以下もう少し例をあげれば

$$a\neq 0 \rightarrow a\cdot a^{-1}=1$$

ここに $a\neq 0$ は正式には $\neg(a=0)$ と書くべきものである．

$$a+(-a)=0$$

$$a\cdot b=b\cdot a$$

$$0^{-1}=0$$

最後は普通には 0^{-1} は定義されないのであるが，ここでは面倒であるのでそ

れを 0 と定義しておく．

上で見られるように，われわれがここで体というのはすべて可換体のことである．体をトリビアルにしないために

$$0 \neq 1$$

なる公理もつけ加えておくことにする．

3.　体の定義

数学的構造　$\langle K, 0, 1, +, \cdot, -, ^{-1} \rangle$

があたえられて，それが体の公理をみたすときに，その数学的構造を**体**という．これが正式の体の定義である．もう少し説明すると，上で K は集合，$0, 1$ は K の特別な元，$-$ と $^{-1}$ とは K の上に定義された 1 変数の演算，$+$ と $\cdot$ とは K の上に定義され，その値がふたたび K の元になるような変数の演算（関数といってもよい）であって，それが体の公理をすべてみたしているとき，この数学的構造を体というのである．しばしば単に K を体といい，体 K というようないい方をするが，正確には

$$\mathcal{K} = \langle K, 0, 1, -, ^{-1}, +, \cdot \rangle$$

とおいて $\mathcal{K}$ を体，K を体 $\mathcal{K}$ の **underlying set** というのである．

以上の定義がわれわれの常識的な体の定義と同じものであることに異議はないであろう．

以上において，体の特別な元を表わす記号は，0 と 1 としか用いなかったが，そのほか π とか e とか好きなだけ増してもよい．ここで π や e が解析学の π や e を表わすためのものであっても，それに無関係なものであってもここまでの話は一向にかかわりはない．π や e を単なる記号として考えるだけのことであるから，そしてそれについての公理を何一つ加えない以上は別に何の意味ももたないのである．一般に K の特別な元を表わす記号を

$$c_1, c_2, \cdots$$

というふうにたくさんつけ加えておくこともある．このときはわれわれの言

語はもとの言語より広くなっているので，もとの言語を L と書くとき，こうやって拡大された言語のことを

$$L\{c_1, c_2, \cdots\}$$

というふうに書くのである．

もちろんこの場合はこの拡大された言語の term の定義も拡大されるべきで，term の定義の 1）はつぎの 1′）でおきかえられる．

1′）　特別な元を表わす記号および変数は term である．

4.　完全性定理

上に体の公理についてのべたが，一般に命題の集合があたえられたとき一つの**公理系**があたえられたという．１つの**理論**（theory）があたえられたというふうにいうこともある．

１つの公理系から論理の推論によって得られた命題をその公理系（または理論）の**定理**という．またはその命題がこの公理系で**証明**できるという．

矛盾が証明されない公理系のことを**無矛盾**な公理系という．矛盾が証明されればすべての命題が証明されてしまうから矛盾の証明される公理系はあまり意味がない．

いまある公理系 $\mathfrak{T}$ と数学的構造 $\mathfrak{S}$ とがあたえられたとするとき，$\mathfrak{T}$ のすべての公理が $\mathfrak{S}$ の上で成立するとき，$\mathfrak{S}$ は $\mathfrak{T}$ の**モデル**である，という．$\mathfrak{S}$ が $\mathfrak{T}$ のモデルであるとき，$\mathfrak{S}$ の上で $\mathfrak{T}$ の定理は明らかにすべて成立する．

いま公理系 $\mathfrak{T}$ がモデル $\mathfrak{S}$ をもつとき，$\mathfrak{S}$ の上で矛盾が成立することはありえないから，$\mathfrak{T}$ から矛盾がでてこないことがわかる．これをいい直すとつぎの定理となる．

定理 1　公理系 $\mathfrak{T}$ がモデルをもてば，$\mathfrak{T}$ は無矛盾である．

この定理の逆がゲーデルの**完全性定理**（completeness theorem）といわれているものでつぎの定理である．

定理 2　公理系 $\mathfrak{T}$ が無矛盾であれば，$\mathfrak{T}$ をみたすモデルが存在する．

ここではその証明は省略するが，これがロジックで最初の定理らしい定理といってよいだろう．

この定理のちょっとした応用としてつぎの定理を証明しておくことにする．

定理 3 (compactness theorem) いま公理系 $\mathfrak{T}$ のすべての有限個の公理にモデルが存在すれば，$\mathfrak{T}$ 自身がモデルをもつ．

(証明)　上の定理によって $\mathfrak{T}$ が無矛盾であることのみを証明すればよい．ところで $\mathfrak{T}$ から矛盾が論理的に証明されるならば，その証明のなかでわれわれは $\mathfrak{T}$ の内の有限個の公理だけを用いているわけである．（すべての証明は有限回の推論で行なわれる．したがってその内で用いられる仮定は高々有限個である．）すなわちこの有限個の $\mathfrak{T}$ の公理から矛盾がでたわけであるが，これはこの有限個の公理がモデルをもつことに反する．

以上の定理の簡単な応用として，つぎの定理が証明される．

定理 4　いま高々可付番個の構成員（ということは高々可付番個の特別な元を表わす記号，関数記号，命題記号しかもっていないということ，いまのわれわれの体の言語の場合は正しくそうである）からなっている言語のある公理系 $\mathfrak{T}$ に対してある無限のモデル M_0 が存在したとする．このとき任意の無限濃度 κ に対して $\mathfrak{T}$ のモデル M で M の濃度が κ であるようなものが存在する．

(証明)　いまもともとの高々可付番の言語を L とする．いま L に新しい記号 $c_0, \cdots, c_\alpha, \cdots$ $(\alpha<\kappa)$ をつけ加えて拡大してできた言語

$$L\{c_0, \cdots, c_\alpha, \cdots\}$$

を考える．いま公理系 $\mathfrak{T}$ につぎの公理をつけ加えて拡大したものを $\tilde{\mathfrak{T}}$ とする．

$$c_\alpha \neq c_\beta \text{（すべての } \alpha, \beta<\kappa \text{ で } \alpha\neq\beta \text{ なるもの全部について考える）}$$

いま $\tilde{\mathfrak{T}}$ の有限個の公理をとって考えると，それは $\mathfrak{T}$ の有限個の公理のほかは

$$c_{\alpha_i} \neq c_{\alpha_j} \qquad (i, j=1, \cdots, n \text{ で } i\neq j)$$

という形だと思ってさしつかえない．

ところで M_0 は無限であるから n 個の相異なる点 m_1, …, m_n をとってきて，

$$c_{\alpha_i} \text{ が } m_i \text{ を意味する}$$

ものと考えれば，M_0 はこの有限個の公理のモデルになっている．したがって定理 3 によって $\tilde{\mathfrak{T}}$ のモデルが存在する．このモデルを M_1 と書くことにしよう．M_1 で c_α の表わす元を m_α とすれば，M_1 は

$$c_\alpha \neq c_\beta \qquad (\alpha \neq \beta, \alpha, \beta < \kappa)$$

のモデルであるから　$m_\alpha \neq m_\beta \ (\alpha \neq \beta, \alpha, \beta < \kappa)$

となる．すなわち M_1 には少なくとも κ 個の元が存在する．すなわち

$$\overline{\overline{M}}_1 \geqq \kappa$$

であり，さらに M_1 は $\tilde{\mathfrak{T}}$ のモデルであるから，もちろん $\mathfrak{T}$ のモデルである．

いま M_1 の部分集合 M_2 を上手にとれば $\overline{\overline{M}}_2 = \kappa$ であって M_2 が $\mathfrak{T}$ のモデルであるようにできることを証明しよう．

まず最初に

$$L\{c_0, \cdots, c_\alpha, \cdots\} = L_0$$

とおこう．

L_0 の構成員の濃度は明らかに κ である．だから L_0 の命題全体の集合の濃度はやはり κ である．

この L_0 の命題のなかで M_1 で正しいもので存在記号からはじまる命題を全部並べて

$$\exists x A_0'(x), \exists x A_1'(x), \cdots, \exists x A_\alpha'(x), \cdots \ (\alpha < \kappa)$$

とする．これに対して新しい記号

$$c_0', \cdots, c_\alpha', \cdots \ (\alpha < \kappa)$$

を導入して，

$$L_1 = L_0\{c_0', \cdots, c_\alpha', \cdots\}$$

とし，$\mathfrak{T}_1$ を $\mathfrak{T}$ と $A_0'(c_0'), A_1'(c_1'), \cdots, A_\alpha'(c_\alpha'), \cdots$ とを一緒にしてできたものとする．M_1 は

$$\exists x A_0'(x), \exists x A_1'(x), \cdots, \exists x A_\alpha'(x), \cdots \ (\alpha < \kappa)$$

のモデルであるから，M_1 の元 $\bar{c}_0', \cdots, \bar{c}_\alpha', \cdots$ で M_1 で

$$A_0'(\bar{c}_1'),\cdots,A_\alpha'(\bar{c}_\alpha'),\cdots$$

がすべて成立するようにできる．いまこの $\bar{c}_\alpha'$ が c_α' が M_1 で表わす元であると定義して M_1 を L_1 に対して拡大し，そしてできたものを同じ M_1 で表わす．

さて L_1 の命題で（こうして拡大された）M_1 で正しく存在記号ではじまるものの全体を並べて

$$\exists x A_0''(x),\exists x A_1''(x),\cdots,\exists x A_\alpha''(x),\cdots\quad(\alpha<\kappa)$$

としてこれに対して $c_0'',\cdots,c_\alpha'',\cdots$ を導入し

$$L_2=L_1\{c_0'',\cdots,c_\alpha'',\cdots\}$$

$\bar{c}_0'',\cdots,\bar{c}_\alpha'',\cdots$ なる $c_0'',\cdots,c_\alpha'',\cdots$ の M_1 で表わす元は $A_0''(\bar{c}_0''),\cdots,A_\alpha''(\bar{c}_\alpha''),\cdots$ が M_1 で成立するようなものを1つとってきて定義することとする．

このようにして，一般に

$$c_0^{(n)},\cdots,c_\alpha^{(n)},\cdots\quad(\alpha<\kappa)$$

を導入し

$$\bar{c}_0^{(n)},\cdots,\bar{c}_\alpha^{(n)},\cdots\quad(\alpha<\kappa)$$

を M_1 の元として定義することができる．いま

$$M_2=\{\bar{c}_0,\cdots,\bar{c}_\alpha,\cdots,\bar{c}_0^{(n)},\cdots,\bar{c}_\alpha^{(n)},\cdots\}_{\substack{n<\omega\\ \alpha<\kappa}}$$

と定義すれば，L_n の命題 A が M_1 で成立することと，M_2 で成立することが同等であることが，A のなかの論理記号の数についての数学的帰納法によって容易に証明することができる．ところで M_1 は $\mathfrak{T}$ のモデルであるから M_2 も $\mathfrak{T}$ のモデルであり，

$$\overline{\overline{M}}_2=\kappa$$

は明らかであるから，定理は証明された．

5.　代数的閉体

体 K が**代数的閉体**であるというのは，その体のなかでどんな方程式を考えても必ず根がその K の元のなかに存在することである．もう少しくわしくいえば

$$x^n+a_1x^{n-1}+\cdots+a_n=0$$

なる勝手な方程式を考えることにする．ここに $a_1, \cdots, a_n$ は K の元であるとする．このとき $x \in K$ でこの方程式の根であるような x が見つかることである．さらにキチンと表現すれば

$$\mathrm{AC}: \quad \forall a_1, \cdots, a_n \exists x (x^n + a_1 x^{n-1} + \cdots + a_n = 0)$$

なる形の命題がすべての $n=1,2,3,\cdots$ に対して K の上で成立していることである．いま上に AC と書いたのは algebraically closed の略で，これは $n=1,2,3,\cdots$ と無限に多くの命題を意味している．

いま代数的閉体についてのわれわれの定理をのべるために 2，3 の論理学の用語を説明しよう．

いまある公理系 $\mathfrak{T}$ があたえられたとき，$\mathfrak{T}$ が**完全** (complete) であるというのは，いま $\mathfrak{T}$ を考えている言語のいかなる命題 A をもってきても，A か $\neg A$ のいずれかが $\mathfrak{T}$ から証明されることをいう．

いまある理論 $\mathfrak{T}$ に対して**決定問題が解ける**というのは，この理論の言語に属するどんな命題 A があたえられても，A か $\neg A$ かいずれかが正しいエフェクティブな方法を見つけることができることをいう．ここでエフェクティブな方法というのはロジックでの帰納的関数というものであるが，だいたいにおいて理想的なコンピューターにキチンとしたプログラムをあたえて，A か $\neg A$ かどちらかを有限個で決定できることだと思えばよい．

いま完全な公理系 $A_0, A_1, \cdots$ でこの公理を全部書き表わすことがエフェクティブにできているような公理系 $\mathfrak{T}$ があたえられたとする．(たとえばわれわれは体の公理群は全部完全に書きつくす（有限個で）ことができる．さらに上の AC を加えても，やはりエフェクティブに全部書き下すことができることは明らかであろう.) このときわれわれはこの公理系の決定問題を解くことができる．これはつぎのようにやればよい．まず $A_0, A_1, \cdots$ から得られる定理を全部書き並べていくプログラムを作る．これは論理学のルールをわれわれは全部書き並べることができるから別にむずかしくはない．いま任意の命題 A があたえられたとき A か $\neg A$ が，この全部の定理の内に現われるか順々に確かめるプログラムを作ればよい．公理系は完全である

から有限回のうちには必ずコンピューターはストップして解答が得られるわけである.

したがってある理論の決定問題はその理論のうまい公理系を見つけてそれが完全であるということを証明するという問題に還元されるのである.

いまわれわれのやろうとすることは，代数的閉体の理論の決定問題を解こうということである．したがってうまい代数的閉体の公理系を提出してそれが完全であるということを証明しようというのである.

だいたいの考えをのべると，体の公理に上の AC をつけ加えたものを公理系としてとればよい．ところで体の理論の初歩を知っている人には上の考えが不十分であることは明らかである．体には標数というものがあって，上の公理からその体の標数が何かわからないことは明白だからである．まず標数が 0 であることはどうやって表わしたらよいであろうか？　これはつぎの公理によって表わされる.

$$C_0:\quad 1+1\neq 0, 1+1+1\neq 0, \cdots, \underbrace{1+\cdots+1}_{n}\neq 0, \cdots$$

ここにやはり $n=2, 3, 4, \cdots$ で C_0 は無限に多くの公理からなっているわけである.

つぎに標数 p(p：素数) というのはどう表わしたらよいであろうか？ これはつぎの公理によって表わされる.

$$C_p:\quad \underbrace{1+1+\cdots+1}_{p}=0,\quad \underbrace{1+\cdots+1}_{p\text{より少ない数}}\neq 0$$

すなわち C_p はここでは有限個の公理からなっているわけである.

ここでのわれわれの定理はつぎのものである．いま p を 0 か，ある特定な素数の 1 つかに決めたときにつぎの定理が成立する.

定理 5　体の公理群と AC と C_p とあわせてできた公理系は完全である.

この定理の証明をするために代数的閉体についての常識を少しばかり解説することにする．いま勝手な体 K があたえられて，その濃度が κ であったとする．いま κ より小さくない無限の濃度 λ (すなわち $\kappa\leqq\lambda$) があたえられたとき，K の拡大体 $\tilde{K}$ で

1) $\tilde{K}$ は代数的閉体

2) $\tilde{K}$ の濃度は λ である

の 2 つの条件をみたすものが存在する．

これは $\lambda=\kappa$ のときは，K の方程式すなわち

$$x^n+a_1x^{n-1}+\cdots+a_n=0$$

で $n=2,3,\cdots$, $a_1,\cdots,a_n\in K$ なるものの濃度はちょうど κ であるから，それを全部並べておいて，順々に必要な根がもしあればそれをつけ加える代数拡大を行なっていき超限帰納法にしたがって次第に大きな拡大体を作ってゆき最後にその和集合をとればよい．1 つの方程式からは高々有限個の根しかでないから，このようにしてできたものが同じ濃度であることは明らかである．

つぎに $\kappa<\lambda$ のときは最初に λ 個の互いに独立な超越元をつけ加えて体を拡大しておいてから，いまと同じことを行なえばよい．λ 個の互いに独立な超越元を K につけ加えてできる体の濃度は明らかに λ であるから，上の事実は明らかに成立する．

つぎに，K^1, K^2 が同じ標数 p ($p=0,2,3,\cdots$) の代数的閉体であってその濃度がともに $\aleph_1$ であったとする．このとき K^1 と K^2 とはまったく同型の体になることがつぎのようにわかる．

われわれは K^1 と K^2 との間の同型写像を作ればよい．このために K^1 と K^2 との元を全部並べて

$$K^1:\ x_0,\cdots,x_\alpha,\cdots\ (\alpha<\omega_1)$$

$$K^2:\ y_0,\cdots,y_\alpha,\cdots\ (\alpha<\omega_1)$$

であるようにする．まず k_0 を標数 p の一番小さい体，すなわち $p=0$ のときは有理数体，$p>0$ のときは自然数を mod p で類別してできた体とする．k_0 は K^1 と K^2 と双方に含まれていると考えられる．

まず，$k_0(x_0)=K^1{}_0\subseteq K^1$ をとって考える．

$K^1{}_0$ が k_0 の代数的拡大であるときでも，超越的拡大であるときでも K^2 の部分体 $K^2{}_0$ と

$$\varphi_0:\ K^1{}_0\to K^2{}_0$$

なる同型写像 φ_0 とを見つけることができる．

こんどは
$$K^2{}_0(y_0)=K^2{}_1\subseteq K^2$$
をとって考える．同様の議論によって，$K^1{}_0\subseteq K^1{}_1\subseteq K^1$ なる K^1の部分体 $K^1{}_1$ と
$$\varphi_1:\quad K^1{}_1\to K^2{}_1$$
なる同型写像 φ_1 で φ_0 の拡大になっているようなものをとることができる．かくして，
$$x_0,y_0,x_1,y_1,\cdots,x_\alpha,y_\alpha,\cdots$$
の順に順々と
$$K^1{}_0\subseteq K^1{}_1\subseteq K^1{}_2\subseteq K^1{}_3\subseteq\cdots\subseteq K^1{}_{2\alpha}\subseteq K^1{}_{2\alpha+1}\subseteq\cdots$$
$$K^2{}_0\subseteq K^2{}_1\subseteq K^2{}_2\subseteq K^2{}_3\subseteq\cdots\subseteq K^2{}_{2\alpha}\subseteq K^2{}_{2\alpha+1}\subseteq\cdots$$
$$\varphi_0\subseteq\varphi_1\subseteq\varphi_2\subseteq\varphi_3\subseteq\cdots\subseteq\varphi_{2\alpha}\subseteq\varphi_{2\alpha+1}\subseteq\cdots$$
と作っていくことができる．
$$\varphi=\bigcup_{\alpha<\omega_1}\varphi_\alpha$$
と定義すれば φ が K^1 と K^2 との間の同型写像であることは明らかであろう．

さていよいよ定理 5 の証明をすることにしよう．いま定理 5 の公理系を Γ とおいて，
$$\Gamma \text{ から証明もされず，否定もされない命題 } A$$
があったとする．このとき Γ と A からできた公理系
$$\Gamma\cup\{A\}$$
も，Γ と $\neg A$ からできた公理系
$$\Gamma\cup\{\neg A\}$$
も無矛盾である．したがって $\Gamma\cup\{A\}$ のモデルと $\Gamma\cup\{\neg A\}$ のモデルが存在する．この2つのモデルはともに代数的閉体であるから，ともに無限に多くの元をもっている．ゆえに定理4によって $\Gamma\cup\{A\}$ はその濃度が $\aleph_1$ のモデル K^1 をもっており $\Gamma\cup\{\neg A\}$ はその濃度が $\aleph_1$ のモデル K^2 をもっている．ところで K^1, K^2 は Γ のモデルすなわち代数的閉体であるから，
$$K^1 \text{ と } K^2 \text{ とは同型}$$
でなければならない．同型なモデルの上ではまったく同じ命題が成立するか

ら，一方で A が成立し，他方で $\neg A$ が成立するということは

矛盾する．

6. 実閉体

実閉体の定義をするためにはまず順序体の定義をしなければならない．順序体の定義をするために体の言語に $=$ 以外の predicate（述語）$<$ を導入して言語を拡大しなければならない．この新しい言語では，formula の構成についてのルールの 1）はつぎの 1′）に拡張させられる．

1′）　s と t が term であるとき，$s=t$ と $s<t$ はともに formula である．

このうえで順序体の公理系とは，体の公理系に $<$ が線型順序であることおよび

$$\forall x, y\,(0<x \wedge 0<y \ \rightarrow\ 0<x+y \wedge 0<x\cdot y)$$

$$\forall x\,(x<0 \ \leftrightarrow\ 0<-x)$$

$$\forall x, y\,(x<y \ \leftrightarrow\ 0<y-x)$$

をつけ加えたものである．順序体の大小の計算は実数の大小の計算と同じでわれわれはよい直観をもっているから，ここではくわしくのべることなく仮定することにする．もちろんある数学的構造が順序体の公理をみたしているとき，その構造を順序体というのである．順序体の標数が 0 であることは明らかであることをちょっと注意しておく．

実閉体の公理系は順序体の公理系につぎの公理をつけ加えてできたものである．

$$\forall x \exists y\,(x>0 \ \rightarrow\ y^2=x)$$

$$\forall a_1, \cdots, a_n \exists x\,(x^n+a_1x^{n-1}+\cdots+a_n=0)$$

ここで n は $3, 5, 7, \cdots$ とする．

すなわち第 2 の公理はじつは無限に多くの公理を表わしているわけである．ここで n が奇数のときだけ考えるというのが大切で，これが代数的閉体と実閉体とのおもな差になっている．

実閉体についての基本的な性質をのべるために，体についての簡単な補題を 1 つのべておく．

補題　いま K は体で，$f(x)$ は係数が K の元であるような多項式で重根をもっていないとする．K のある代数拡大で $f(x)=0$ の根が $\alpha_1, \cdots, \alpha_n$ であったとする．いま K の元 c をとったとき

$$\alpha_j\alpha_k+c(\alpha_j+\alpha_k)$$

は，j，k が $1\leq j<k\leq n$ なる $\dfrac{n(n-1)}{2}$ の場合をつくすとき，$\dfrac{n(n-1)}{2}$ 個の相異なる値をとるものとする．このとき

$$K(\alpha_1\alpha_2, \alpha_1+\alpha_2)=K(\alpha_1\alpha_2+c(\alpha_1+\alpha_2))$$

(証明)

$$\gamma_{jk}=\alpha_j\alpha_k, \qquad \beta_{jk}=\alpha_j+\alpha_k,$$

$$\gamma=\gamma_{12}=\alpha_1\alpha_2, \qquad \beta=\beta_{12}=\alpha_1+\alpha_2, \qquad \theta=\gamma+c\beta$$

とおくことにする．

$K(\gamma, \beta)=K(\theta)$ が証明したいことである．いま

$$F(x)=\prod_{1\leq j<k\leq n}(x-\gamma_{jk})$$

$$G(x)=\prod_{1\leq j<k\leq n}(x-\beta_{jk})$$

とおけば明らかに，$F(x)$ も $G(x)$ もともに K の多項式である．したがって

$$F(\theta-cx)=0$$

$$G(x)=0$$

の 2 つの方程式は明らかに $K(\theta)$ の元を係数とする方程式である．ところで β は明らかにこの 2 つの方程式の共通根になっている．いま β の他にこの 2 つの方程式の共通根がないことを証明しよう．$G(x)=0$ の根の全体は β_{jk} $(1\leq j<k\leq n)$ であるから β_{12} 以外の β_{jk} が $F(\theta-cx)=0$ の根になりえないことをいえばよいが，これは補題の条件から明らかである．ゆえに $(x-\beta)$ は $F(\theta-cx), G(x)$ の最大公約数をユークリッドの互除法を用いることによって得られる，すなわち $K(\theta)$ の多項式となる．ゆえに

$$\beta\in K(\theta)$$

となり，

$$\gamma\in K(\theta)$$

もでる．

いま K を実閉体として，それに

$$i^2=-1$$

なる i を添加してできる代数拡大 $K(i)$ を考えよう．われわれは 2 次方程式，および普通の i の計算はよく知っているから $K(i)$ ですべての 2 次方程式が根をもつことは明らかであろう．これを用いてつぎの定理を証明する．

定理 6 K が実閉体であるとき，$K(i)$ は代数的閉体である．

(証明) $K(i)$ は K の代数拡大であるから，K のすべての既約多項式が $K(i)$ で根をもつことをいえば十分である．われわれはこれをつぎの形で証明する．

$f(x)$ は重根をもたない K の次数 n の多項式であるとき，$f(x)$ は $K(i)$ で根をもつ．

いま

$$n=2^m q$$

で q は奇数であるとして，この命題を m についての数学的帰納法で証明する．

$m=0$ のときは，K が実閉体であるから明らかである．いま $m-1$ のところまでできたと仮定して m の場合を証明することにする．

いま K を適当に代数拡大してそのなかで $\alpha_1,\cdots,\alpha_n$ が $f(x)$ の n 個の根であるとする．いま K には無限に多くの元があるから

$$\alpha_j\alpha_k+c(\alpha_j+\alpha_k) \qquad 1\leq j<k\leq n$$

なる $\dfrac{n(n-1)}{2}$ 個の元が互いに相異なるような $c\in K$ が存在する．ところで

$$\prod_{1\leq j<k\leq n}(x-(\alpha_j\alpha_k+c(\alpha_j+\alpha_k)))$$

なる多項式を考えると，これは明らかに K の元を係数とする多項式でさらにその次数は $\dfrac{n(n-1)}{2}$ である．

$$\frac{n(n-1)}{2}=2^{m-1}\cdot q\cdot(2^m\cdot q-1)$$

であるから，帰納法の仮定により，この多項式は $K(i)$ に根をもつ．いまそ

の根になるものを，一般性を失わないから

$$\alpha_1\cdot\alpha_2+c(\alpha_1+\alpha_2)$$

とする．

補題によって
$$\alpha_1\cdot\alpha_2\in K(i)$$
で
$$(\alpha_1+\alpha_2)\in K(i)$$
がわかる．2 次方程式は $K(i)$ で解をもつから，

$$\alpha_1\in K(i)$$
$$\alpha_2\in K(i)$$

がいえて定理が証明された．

この定理を用いてつぎのよく知られた定理を証明する．

定理 7　K を実閉体とするとき，K の多項式は 1 次式と 2 次式とに因数分解される．

（証明）　いま K の任意の多項式を $f(x)$ とする．前定理により $f(x)$ は $K(i)$ に根をもつ．それを

$$a+bi,\qquad a\in K, b\in K$$

としよう．もし
$$b=0$$
ならばこれは $(x-a)$ なる 1 次の因数をもつ．いま
$$b\neq 0$$
とすれば
$$x-(a-bi)$$
がやはり $f(x)$ の因数になることは容易にわかる．

ゆえに
$$(x-(a+bi))(x-(a-bi))=x^2-2ax+(a^2+b^2)$$
が $f(x)$ の因数になっていることがわかる．あとは普通のように因数分解を続けていけば定理は明らかである．

定理 8　K を実閉体とし $K(x)$ を順序体としての K の超越拡大とする．いまもし K のすべての元 a について

$$a\leq x \quad か \quad x\leq a$$

かが決定されれば，$K(x)$ の上の順序 $<$ はすべて決定される．

(証明) $K(x)$ の0以外の元の正，負が決定されることをいえばよい．t を $K(x)$ の任意の元とすれば

$$t=a\cdot\frac{a_0+a_1x+\cdots+x^k}{b_0+b_1x+\cdots+x^m},\qquad k\geq 0, m\geq 0$$

で
$$a, a_0, a_1, \cdots, b_0, b_1, \cdots \in K$$

である．前定理によって，これは

$$t=a\cdot\frac{\prod(x-c_j)\prod((x-d_j)^2+e_j{}^2)}{\prod(x-c_j')\prod((x-d_j')^2+e_j'^2)}$$

の形に書ける．$(x-d)^2+e^2$ の形は負にならないから，この t の正負は a, $(x-c_j)$, $(x-c_j')$ の正負だけで決定される．すなわち定理が得られた．

7. 関数記号の除去

論理学では，関数記号が便利なときは関数記号を用い，不便なときは用いない．とったり，つけ加えたりするのである．これについて一般論を堂々と展開することができるが，実際には常識にしたがってただものをキチンと書いていくだけのことである．だいたいのアイディアをのべるとつぎのようになる．

いま
$$\forall x_1, \cdots, x_n \exists y A(x_1, \cdots, x_n, y)$$

という公理があたえられていたとする．このとき，都合によっては，f という新しい関数記号を言語に導入して上の公理を

$$\forall x_1, \cdots, x_n A(x_1, \cdots, x_n, f(x_1, \cdots, x_n))$$

という形に変形するのである．一般に公理をのべるのに，簡単な変形によって，$\forall$ や $\exists$ がすべてその公理の一番はじめにだけあるようにできるから，この方法を何度もくり返すことによって公理系の形を変形して $\exists$ が1つも用いられてなくて，$\forall$ が公理の一番はじめにだけあるようにすることができる．こういう形は一般には新しい関数記号をたくさん導入することになるが，公理系のとり扱いに便利なことが多い．

つぎに関数記号が邪魔になってとりのぞきたいときがある．このときはつぎのようにやるのである．

われわれのとり扱っている言語のなかの任意の関数記号 f について，新しい predicate P を言語に導入する．ここで f が n 変数ならば P は $n+1$ 変数とするのである．

いま P についての新しい公理

$$\forall x_1, \cdots, x_n \exists! y\ P(x_1, \cdots, x_n, y)$$

というのを導入する．ここで $\exists! y$ は‘ただ 1 つの y が存在する’と読むのであって，一般に

$$\exists! y A(y) \quad は \quad \exists y A(y) \wedge \forall u, v(A(u) \wedge A(v) \rightarrow u=v)$$

の略であると思うのである．

この形の公理を導入したうえで，たとえば古い公理のなかに関数記号の入っているところをつぎの手続きで少しずつ変形していくのである．

$R(f(t_1, \cdots, t_n), s_2, \cdots, s_m)$ というところを $\exists y(P(t_1, \cdots, t_n, y) \wedge R(y, s_2, \cdots, s_m))$ とかえる．

たいていの場合は $t_1, \cdots, t_n, s_2, \cdots, s_m$ のなかにまだ関数記号が残っているから，この手続きをくり返しくり返し用いることになる．また関数記号をとりのぞくためには新しい predicate の導入のみならず，公理を変形していくときに新しい $\forall$ や $\exists$ がイッパイ入ってくるのである．こうして

$$関数記号のある体系 \rightleftarrows 関数記号のない体系$$

と 2 つの矢印が変形という手続きという意味で定義されたわけであるが，こうして互いに移行する 2 つの公理系がじつは同等であるということも容易に証明される．これはもちろん公理系の同等ということを定義して，それから厳密に運ぶのでいかにも定理らしくなるが実際には常識以外の何物でもない．細かい技術的な面に関心のある読者は小著『数学基礎論』（共立）でも見られたい．

さてこの流儀で順序体および実閉体から関数記号をとり去るとしたらどうなるであろうか？　われわれの言語の関数記号は $+, \cdot, -, ^{-1}$ と 4 つであるから原則としては 4 つ新しい predicate を導入すべきである．しかし，それは実際には必要がない．なぜならば，$-$ と $^{-1}$ はもともと逆元であって

それを用いなくても

$$\forall x(x \neq 0 \rightarrow x \cdot x^{-1}=1) \quad \text{は} \quad \forall x \exists y(x \neq 0 \rightarrow x \cdot y=1)$$

と書けばよいところを無精のために $^{-1}$ を入れておいた，というところであり，$-$ や $^{-1}$ のない公理系のほうがむしろ常用のものであるからである．

したがっていまわれわれの場合は $+$ と $\cdot$ についての新しい predicate を導入すればよい．すなわち S と P とを導入する．S は sum の略であり，P は product の略である．すなわち以下において

$$S(a,b,c), P(a,b,c) \text{ はそれぞれ } a+b=c, a\cdot b=c \text{ を表わす}$$

ものと思ってよい．ところで S や P はピンとこないので，やはり前と同じく $a+b=c, a\cdot b=c$ を用いたりする．しかしこんどは，これは $S(a,b,c)$ や $P(a,b,c)$ の略なのであって，$+$ や $\cdot$ なる関数記号があるわけではない．したがって一般に term なるものは，0, 1 か変数しかないことになっており，$a+b=c, a\cdot b=c$ と書いても a,b,c は変数か 0, 1 を表わしてよいのである．

もう 1 つこの機会に断っておきたいのは，われわれは $<$ を基本的な記号として採用した．その際は

$$a \leq b \quad \text{は} \quad a<b \vee a=b \quad \text{の略}$$

と定義するのであるが，逆に $\leq$ を基本的な記号と採用して

$$a<b \quad \text{は} \quad a \leq b \wedge a \neq b \quad \text{の略}$$

と定義してもよい．こんなツマラないことを注意するのは，本や論文によって著者が自分の好きなほう（または偶然によって選ばれたほう）を用いるのであまり読者が自分流に決めてしまうと困ることがあることをいっておきたかったのである．

とにかく，以下において，われわれの体系には関数記号はなく，predicate は $=$，$<$，S，P の 4 つだけであることを断っておきたい．

8. elementary extension

タルスキーの定理の証明をのべる前に，論理学の重要な概念 elementary extension についてのべておきたい．

定義　k が順序体，K が順序体としての k の拡大体であるとする．このとき K が k の elementary extension であるというのは，順序体の言語のなかの任意の formula $A(x_1, \cdots, x_n)$ と k の元 $a_1, \cdots, a_n$ とをとってきたとき $A(a_1, \cdots, a_n)$ が k で成立することと $A(a_1, \cdots, a_n)$ が K で成立することとが，同等なことを意味する．ここに $a_1, \cdots, a_n \in k$ のとき $A(a_1, \cdots, a_n)$ なる形を k **についての命題**ということにする．

ここでちょっと例をあげることにすれば，いまもし K が k の elementary extension であったとする．そして $a_1, \cdots, a_n \in k$ のとき

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

なる方程式が K で根をもったとする．これを論理的に表現すれば

$$K \text{ で } \exists x(x^n + a_1 x^{n-1} + \cdots + a_n = 0) \text{ が成立する}$$

ということになる．ところでこれは $A(a_1, \cdots, a_n)$ なる形の命題で，$a_1, \cdots, a_n \in k$ であるから，K が k の elementary extension という仮定から

$$\exists x(x^n + a_1 x^{n-1} + \cdots + a_n = 0) \text{ は } k \text{ でも成立}$$

する．すなわち $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ は k で根をもつ．この例は elementary extension という概念が大切であることを明白に物語っている．

ここしばらくの目標はつぎの定理である．

定理 9　k，K はともに実閉体であって，K は k の拡大体である．このとき K は k の elementary extension である．

ここで K が k の拡大体であるとしかいわないで，順序体として拡大体であるとウルサクいわなかったのは，実閉体では順序は 0 でない 2 乗の形で表わされるものが正というふうに簡単に代数的に定義されてしまうので，必要がないからである．

さてこの定理を証明するために少し準備をすることにする．

定義　ある formula が順序体 k の $\exists$—$\wedge$ 形であるというのはその formula が

$$\exists y_1, \cdots, y_n (P_1(y_1, \cdots, y_n) \wedge \cdots \wedge P_m(y_1, \cdots, y_n))$$

の形で，ここに $P_i(y_1, \cdots, y_n)$ は

$$a=b,\quad a\neq b,\quad a<b,\quad a\leq b,\quad S(a,b,c),$$
$$\neg S(a,b,c),\quad P(a,b,c),\quad \neg P(a,b,c)$$

のいずれかの形である．ここで a,b,c は k の元かまたは $y_1,\cdots,y_n$ の 1 つである．

以下には $S(a,b,c)$，$\neg S(a,b,c)$，$P(a,b,c)$，$\neg P(a,b,c)$ のかわりに

$$a+b=c,\quad a+b\neq c,\quad a\cdot b=c,\quad a\cdot b\neq c$$

と書くことにする．

さて定理 9 を証明するためにまずそれよりは少し弱いつぎの定理を証明する．

定理 10 k,K は実閉体で K は k の拡大体であるとする．いま A が k の $\exists$—$\wedge$ 形であるとき，k で A が成立する必要十分条件は K で A が成立することである．

（証明）いま A を $\exists y_1,\cdots,y_n B(y_1,\cdots,y_n)$ とするとき A が k で成立するということは，k の元 $a_1,\cdots,a_n$ があって $B(a_1,\cdots,a_n)$ が k で成立するということである．いま B のなかに $\forall$ か $\exists$ は 1 つもないから，また K は k の拡大体であるから，$B(a_1,\cdots,a_n)$ は K で成立する．すなわち　A は K で成立する．

したがってわれわれが証明すべきことは A が K で成立することを仮定して，A が k でも成立することを証明すればよい．

いま　A が K で成立していたとする．これは K の元 $b_1,\cdots,b_n$ が見つかって，

$$B(b_1,\cdots,b_n)\text{ が } K \text{ で成立}$$

することである．いま k の拡大体 $k(b_1,\cdots,b_n)$ を作り，それを含む最小の実閉体を k^* とする．

$$B(b_1,\cdots,b_n)\text{ が } k^* \text{ で成立}$$

することは明らかである（B に $\forall$ や $\exists$ が 1 つもないから）．いま k^* の k の上の超越次元は高々 n であるから

$$k=k_0\subseteq k_1\subseteq k_2\subseteq\cdots\subseteq k_n=k^*$$

であるような実閉体 k_i を作って

$$k_{i+1} \text{ の } k_i \text{ の上の超越次元が高々 } 1$$

であるようにできる．いま A が k で成立することをいうために k_n から順順に $k_{n-1},\cdots$ と k_i の上で A が成立することを証明していく．だからはじめから K が k の上の超越次元が高々 1 の拡大であると考えて定理を証明すればよい．最初に　　　　超越次元が 0

であるとすると，K は定理 7 により，k に 2 次式の根をいくつかつけてできたものでなければならない．しかもこの 2 次式は

$$(x-c)^2+d^2 \qquad c, d\in k$$

の形であることがわかっているから，このような 2 次式の根をつけ加えるということと $i^2=-1$ なる i をつけ加えるということは実閉体 k の上では同等であるから，これは不可能である．ゆえにこれは

$$K=k$$

を意味することになり定理は明らかである．

よって　　　　K が k の上の超越次元がちょうど 1

であるとして証明すればよい．

いま K の元で k の元とはならないものを 1 つとってきてこれを b としよう．　　　　K は $k(b)$ を含む最小の実閉体

になっているわけである．また k のすべての元についてその元を表わす記号 c_ν を導入しよう．ここで ν は k の濃度より小さいすべての順序数を走るものとする．c_ν の表わす k の元を $\bar{c}_\nu$ と書くことにしよう．

われわれはつぎの公理系を考えよう．

Γ_0：実閉体の公理群

D：$\{c_{\nu_1}\neq c_{\nu_2} \mid \nu_1\neq\nu_2\}$

$\cup\{c_{\nu_1}<c_{\nu_2} \mid \bar{c}_{\nu_1}<\bar{c}_{\nu_2}$ が k で成立しているとき$\}$

$\cup\{c_{\nu_1}+c_{\nu_2}=c_{\nu_3} \mid \bar{c}_{\nu_1}+\bar{c}_{\nu_2}=\bar{c}_{\nu_3}$ が k で成立しているとき$\}$

$\cup\{c_{\nu_1}+c_{\nu_2}\neq c_{\nu_3} \mid \bar{c}_{\nu_1}+\bar{c}_{\nu_2}\neq\bar{c}_{\nu_3}$ が k で成立しているとき$\}$

$\cup\{c_{\nu_1}\cdot c_{\nu_2}=c_{\nu_3} \mid \bar{c}_{\nu_1}\cdot\bar{c}_{\nu_2}=\bar{c}_{\nu_3}$ が k で成立しているとき$\}$

$\cup\{c_{\nu 1}\cdot c_{\nu 2}\neq c_{\nu 3}\mid \bar{c}_{\nu 1}\cdot \bar{c}_{\nu 2}\neq \bar{c}_{\nu 3}$ が k で成立しているとき$\}$

H: $\{c_\nu < c \mid \bar{c}_\nu < b$ が K で成立しているとき$\}$

$\cup\{c < c_\nu \mid b < \bar{c}_\nu$ が K で成立しているとき$\}$

$\cup\{c\neq c_\nu \mid$ すべての c_ν について$\}$

いまわれわれは A が $\Gamma_0\cup D\cup H$ なる公理系から証明ができることを証明する．いまもしそうでないとすると

$\Gamma_0\cup D\cup H\cup\{\neg A\}$ はモデル K' をもつ．

$\neg A$ は $\forall y_1,\cdots,y_n \neg B(y_1,\cdots,y_n)$

の形である．K' で c の表わす元を b' とする．K' のなかで c_ν の表わす元を $\bar{c}_\nu$ と同一視すれば

K' は k の拡大順序体

であると思ってよい．さらに K' は Γ_0 をみたすから

K' は実閉体

である．いま $k(b')$ を考えれば定理 8 により

$k(b)$ も $k(b')$ も H のモデル

であるから　　$k(b')$ は $k(b)$ と順序体として同型

である．いま K'' を K' のなかでの $k(b')$ を含む最小の実閉体とすれば K'' と K とはそれぞれ $k(b')$ と $k(b)$ とを含む最小の実閉体であるから

K'' と K とは同型

である．ゆえに　　K'' で A が成立

する．ところで K'' の拡大体 K' で $\forall y_1,\cdots,y_n \neg B(y_1,\cdots,y_n)$ が成立して B のなかには $\forall$ や $\exists$ がないから，

K'' でも $\forall y_1,\cdots,y_n \neg B(y_1,\cdots,y_n)$ が成立

しなければならない．ところでこれは $\neg A$ であるから K'' で A が成立することに　　矛盾する．

さて A が $\Gamma_0\cup D\cup H$ から証明されることがわかった．ところですべての証明は有限回の操作でなされるから H のなかの有限個の公理だけが用いられる．これを並べて　　$C_1(c),\cdots,C_m(c)$

とする．

この証明は $\Gamma_0 \cup D$ と $C_1(c) \wedge \cdots \wedge C_m(c)$ から A が証明された証明と思ってよい．

ところで Γ_0, D, A のなかには c は用いられていないから，この c は $C_1(c) \wedge \cdots \wedge C_m(c)$ をみたすものならばどんなものでもよい．したがってこの証明は，

$$\Gamma_0 \cup D \text{ から } \exists y(C_1(y) \wedge \cdots \wedge C_m(y)) \to A$$

がでてくる証明と思ってよい．したがってわれわれは k で A が成立することをいうためには k で $\exists y(C_1(y) \wedge \cdots \wedge C_m(y))$ が成立することをいえばよい．

$$C_1(y) \wedge \cdots \wedge C_m(y)$$

を書き直してみると

$$\begin{aligned} &\bar{c}_1 < c \wedge \cdots \wedge \bar{c}_i < c \\ &\wedge \bar{c}_1{}' \neq c \wedge \cdots \wedge \bar{c}_j{}' \neq c \\ &\wedge c < \bar{c}_1{}'' \wedge \cdots \wedge c < \bar{c}_k{}'' \end{aligned}$$

という形である．いまここで c に b を代入すれば K でこれは正しいものであるから

$$\bar{c} = \max(\bar{c}_1, \cdots, \bar{c}_i) < \bar{c}'' = \min(\bar{c}_1{}'', \cdots, \bar{c}_k{}'')$$

がでてくる．ゆえにいいたいことは k で

$$\exists y(\bar{c} < y \wedge y < \bar{c}'' \wedge y \neq \bar{c}_1{}' \wedge \cdots \wedge y \neq \bar{c}_j{}')$$

が成立することであるが，$\bar{c}$ と $\bar{c}''$ の間に k の元は無限に存在するからこれは証明された．

さていよいよ定理 10 を用いて定理 9 の証明をすることにする．

いま　　　　k，K がともに実閉体で K が k の拡大体

であるとする．いまさらに

$$A \text{ は } k \text{ についての命題}$$

であるとする．

$$\text{‘}A \text{ が } k \text{ で成立する’} \leftrightarrow \text{‘}A \text{ が } K \text{ で成立する’}$$

を A のなかの論理記号の数についての数学的帰納法で証明することにする．

まず A に論理記号が 1 つもないときは明らかである.

いまもし A が $\neg B,\ B\vee C,\ B\wedge C$ のいずれかであれば，帰納法の仮定により，B, C に対してはすでに上の関係が成立しているからAに対しても成立することは明らかである.

あと残るのは A が $\forall xB(x)$ の形のときと $\exists xB(x)$ の形のときであるが，$\forall xB(x)$ の形はすべて $\neg\exists x\neg B(x)$ に変形しておいて $\forall$ は一切用いないことにしておけばよいから（だから帰納法をこういうふうに仮定した上で用いる） A が $\exists xB(x)$ の形のときにだけやればよい.

K が k の拡大体であるから，$\exists xB(x)$ が K で成立しているとき $\exists xB(x)$ がやはり k でも成立していることを証明すればよい.

$\exists xB(x)$ は K で成立するのであるから，K の元 b が存在して $B(b)$ が K で存在する．ところで $B(b)$ の論理記号の数は A の論理記号の数より 1 だけ少ない．すなわち帰納法の仮定により，任意の K の実閉体である拡大体 $\tilde{K}$ をとると

*) ‘$B(b)$ が K で成立する’ $\leftrightarrow$ ‘$B(b)$ が $\tilde{K}$ で成立する’

がなりたつ.

いま K のすべての元を表わす記号を導入して言語を拡大する．（面倒だからここでは K の元と K の元を表わす拡大された言語のなかの記号とを同じ文字を用いて表わすようにする）そしてつぎのごとき公理系を考えることにする.

Γ_0：実閉体の公理

D：$\{d_1<d_2 | d_1, d_2\in K$ で $d_1<d_2$ が K で成立する$\}$

$\cup\{d_1\neq d_2 | d_1, d_2\in K$ で $d_1\neq d_2\}$

$\cup\{d_1+d_2=d_3 | d_1, d_2, d_3\in K$ で $d_1+d_2=d_3\}$

$\cup\{d_1+d_2\neq d_3 | d_1, d_2, d_3\in K$ で $d_1+d_2\neq d_3\}$

$\cup\{d_1\cdot d_2=d_3 | d_1, d_2, d_3\in K$ で $d_1\cdot d_2=d_3\}$

$\cup\{d_1\cdot d_2\neq d_3 | d_1, d_2, d_3\in K$ で $d_1\cdot d_2\neq d_3\}$

ちょっと注意をすれば D の $\{\quad\}$ の内部の | より左側の式は言語のなかの formula としての式であり，同じものが右側に現われた式は K のなかで成立しているという意味なのである．

いまわれわれは　Γ_0, D から $B(b)$ が証明できる

ことをいおう．もし $B(b)$ が Γ_0, D から証明できなければ $\Gamma_0, D, \neg B(b)$ は無矛盾である．ゆえに $\Gamma_0, D, \neg B(b)$ はモデルがある．そのモデルを M とおけば M は Γ_0 のモデルであるから実閉体である．さらに M は D のモデルであるから M は K を部分体としてもっている．ところで M では $B(b)$ は成立しない．これは上にのべた ＊）に反する．

さて $B(b)$ は Γ_0, D から証明されるから Γ_0 と D の有限個から証明される．その有限個を $D_1, \cdots, D_n$ とし $D_1, \cdots, D_n$ のなかに入っている k でない K の元を $b_1, \cdots, b_m$ とする．すなわち $D_1, \cdots, D_n$ を書き直して

$$D_1(b_1, \cdots, b_m), \cdots, D_n(b_1, \cdots, b_m)$$

とする．したがって

$$\Gamma_0 \text{ と } D_1(b_1, \cdots, b_m)\wedge\cdots\wedge D_n(b_1, \cdots, b_m)$$

から　$D(b)$

したがって　$\exists x D(x)$

が証明される．ところで Γ_0 と $\exists x D(x)$ のなかには $b_1, \cdots, b_m$ は現われないから，この証明で $b_1, \cdots, b_m$ は

$$D_1(b_1, \cdots, b_m)\wedge\cdots\wedge D_n(b_1, \cdots, b_m)$$

をみたすものならばどんなものでもよいわけである．したがって

$$\Gamma_0 \text{ と } \exists x_1, \cdots, x_m(D_1(x_1, \cdots, x_m)\wedge\cdots\wedge D_n(x_1, \cdots, x_m))$$

から　$\exists x B(x)$

が証明される．ところで $\exists x_1, \cdots, x_m(D_1(x_1, \cdots, x_m)\wedge\cdots\wedge D_n(x_1, \cdots, x_m))$ は k の $\exists$—$\wedge$ 形であって K で成立するから定理 10 によってこれは k でも成立する．したがって　k で $\exists x B(x)$ が成立

する．

9. タルスキーの定理

いよいよ，実閉体の決定問題を解くことにする．前にいったようにわれわれの公理系が完全であれば決定問題は解けるから，ここではタルスキーの定理をつぎの形で証明することにする．

定理 11 実閉体のわれわれの公理系は完全である．

(証明) われわれの実閉体の公理系を Γ_0 とおくことにする．いま順序体の言語に属する命題 A で

Γ_0 から A も $\neg A$ も証明できない

ものがあったとして矛盾を導くことにする．この仮定により Γ_0 と A とは無矛盾であるから，Γ_0 と A とのモデル K_1 が存在する．すなわち

実閉体 K_1 で A のモデル

であるものが存在する．同様にして

実閉体 K_2 で $\neg A$ のモデル

になるものが存在する．ところでいかなる実閉体も有理数体をその部分体としてもっていることは明らかである．したがっていま実数で代数的な数であるものの全体を K_{RA} とおくことにすれば，K_{RA} は明らかに実閉体であって，K_{RA} はすべての実閉体の部分体になっている．

定理 9 によれば，K_1 が A をみたすゆえ，K_{RA} はやはり A をみたさなければならない．同様にして K_2 は $\neg A$ をみたすので，定理 9 により K_{RA} は $\neg A$ をみたさなければならない．

K_{RA} が A と $\neg A$ とを同時にみたす

ことは不可能であるから　　　　矛盾

が生じた．

10. 応用

ここに応用を 2 つだけすることにする．

最初のものは，代数的閉体の理論の応用である．ここに前にいい忘れたこ

とをつけ加えておく．それは実閉体のところでは elementary extension という形で代数的閉体でやったときより理論がくわしい形でのべられているが，これはもちろん易しい理論代数的閉体の場合はもっと簡単にできるものであるが，くわしくのべなかったまでである．代数的閉体の公理が完全であることから，elementary extension の理論がでることを演習問題だと思ってやってみていただいてもよいし，この問題を頭にえがきながら，以下の話を読んでいただいてもよい．

前に，いま2つの代数的閉体 k_1, k_2 があって，$\bar{\bar{k}}_1=\bar{\bar{k}}_2=\aleph_1$ であるとすると，k_1 と k_2 とは同型となることを証明した．その方法と同じ方法でつぎの定理が容易に得られる．

定理 12　k が体であって，K_1, K_2 が代数的閉体で k は K_1, K_2 の部分体であり，

$$\bar{\bar{K}}_1=\bar{\bar{K}}_2>\max(\omega, \bar{\bar{k}})$$

が成立しているとする．このとき K_1 から K_2 への同型写像 φ で k の上では恒等写像になっているものが存在する．

いまこの定理を応用するためにまずつぎの定義をする．

定義　k が体で，われわれの体の言語には，k のすべての元を表わす記号が入っているものとする．このとき，k の**ダイアグラム**というのは，k の元を表わすすべての記号，c_1, c_2, c_3 について

$$c_1\cdot c_2=c_3,\quad c_1\cdot c_2\neq c_3,\quad c_1+c_2=c_3,\quad c_1+c_2\neq c_3,\quad c_1=c_2,\quad c_1\neq c_2$$

のなかで正しい命題全体の集合である．（すべての可能な $c_1, c_2, c_3\in k$ について考える）．

定理 13　いま k は体でわれわれの言語 L は体の言語に k の元を表わす記号を全部つけ加えてできたものとする．この L の命題 A をとってきて，K が k の拡大体であって代数的閉体であるとき，K で A が成立するための必要十分条件は A が k のダイアグラムと代数的閉体の公理系から（すなわちその内の有限個の公理から）証明できることである．

（証明）　十分なことは明らかであるから，必要なことだけを証明すればよい．

いま k のダイアグラムと代数的閉体の公理とからなる公理系を $\tilde{\Gamma}$ とする．

いま
$$\rightharpoondown A \text{ が } \tilde{\Gamma} \text{ から証明される}$$
ならば，K は $\tilde{\Gamma}$ のモデルであるから，K で $\rightharpoondown A$ が成立して矛盾する．したがって $\tilde{\Gamma}$ から A も $\rightharpoondown A$ も証明されない．したがって
$$\tilde{\Gamma}\cup\{A\} \text{ も } \tilde{\Gamma}\cup\{\rightharpoondown A\} \text{ も無矛盾}$$
である．いま κ を $\max(\omega, \bar{\bar{k}})$ より大きい最初の濃度として，$\tilde{\Gamma}\cup\{A\}$ と $\tilde{\Gamma}\cup\{\rightharpoondown A\}$ の濃度が κ であるモデルを作ってこれをそれぞれ K_1, K_2 とする．このとき K_1, K_2 は代数的閉体であり k を部分体としてもっている．前定理により，K_1 と K_2 とは k を部分体として含んで同型である．したがって言語 K の命題については K_1 と K_2 とはまったく同じものとみなしてさしつかえない．ところで一方で A が成立し他方で $\rightharpoondown A$ が成立することは

矛盾する．

定理 14 k は体であって，われわれの言語 L は体の言語に k のすべての元を表わす記号をつけ加えたものとする．A はこの言語での命題で，K_1, K_2 はともに k の拡大体で代数的閉体であるとする．このとき，つぎのことが成立する．
$$(A \text{ が } K_1 \text{ で成立する}) \leftrightarrow (A \text{ が } K_2 \text{ で成立する})$$

証明は前定理より明らかである．

系 k が体であって，$p_1, \cdots, p_m \in k[x_1, \cdots, x_n]$ とする．このとき $p_1, \cdots, p_m$ が k のある代数的閉体である拡大体 $\tilde{k}$ で共通根をもたないならば，k のいかなる拡大体 K でも $p_1, \cdots, p_m$ は共通根をもたない．

(証明) $p_1, \cdots, p_m$ が共通根をもつというのは，
$$\exists x_1, \cdots, x_n(p_1(x_1, \cdots, x_n)=0 \wedge \cdots \wedge p_m(x_1, \cdots, x_n)=0)$$
と前定理の言語 L で表わされる命題である．いま K の拡大体で代数的閉体となるようなものを $\tilde{K}$ とすると，$\tilde{K}$ と $\tilde{k}$ とには同じ命題が成立するから，$\tilde{K}$ には $p_1, \cdots, p_m$ の共通根はない．したがって，K には $p_1, \cdots, p_m$ の共通根はない．

つぎにヒルベルトの Nullstellensatz と呼ばれるつぎの定理を証明する．

定理 15　k が体で K が k の拡大体で代数的閉体とする．いま $p_1, \cdots, p_m \in k[x_1, \cdots, x_n]$ が K で共通根をもたないとすれば，$q_1, \cdots, q_m \in k[x_1, \cdots, x_n]$ を見つけて

$$p_1 \cdot q_1 + \cdots + p_m \cdot q_m = 1$$

となるようにすることができる．

（証明）　前の系により，$p_1, \cdots, p_m$ は k のいかなる拡大体でも共通根をもたない．いま $p_1, \cdots, p_m$ から生成される $k[x_1, \cdots, x_n]$ のイデアルを I とする．I に 1 が入っていれば定理が証明されたことになるから 1 が入っていないものと仮定すれば，I を（たとえば Zorn の補題によって）拡大して極大イデアル J を作る．$k[x_1, \cdots, x_n]/J$ は k の拡大体であって，ここでは，$p_1, \cdots, p_m$ は共通根をもっているから矛盾する．

つぎに実閉体の公理系が完全であることの応用を考えることにする．まず実閉体の言語は順序体の言語と同じであって，順序体の言語は体の言語に順序 $<$ を加えたものであることに注意しよう．

定義　k を順序体とし，いまわれわれの言語 L は順序体の言語に k のすべての元を表わす記号をつけ加えたものとする．（以下 k について考えるときは常にこの言語——これを L_k と書くことにする——について考える）このとき k のダイアグラムとは k の元を表わすすべての c_1, c_2, c_3 について

$$c_1 + c_2 = c_3, \quad c_1 \cdot c_2 = c_3, \quad c_1 < c_2, \quad c_1 = c_2$$

なる形の命題で k の上で正しいもの全体の集合をいう．

すべての順序体は実閉体に拡大できることと，われわれの実閉体の理論からつぎの定理は明らかであろう．

定理 16　k を順序体とし，A を L_k の命題，K_1, K_2 を実閉体とし，ともに k の順序体としての拡大体であるとする．そのとき

$$(K_1 \text{ で } A \text{ が成立する}) \leftrightarrow (K_2 \text{ で } A \text{ が成立する})$$

系　k が順序体で　　$p(x_1, \cdots, x_n) \in k[x_1, \cdots, x_n]$

とする．K は k の順序体としての拡大体でしかも実閉体であるとする．いま $p(x_1, \cdots, x_n)$ が $x_1, \cdots, x_n$ が K のいかなる値を動いても正または 0 であったとするとき，k のいかなる順序体としての拡大体 $\tilde{k}$ をとっても，$\tilde{k}$ で $p(x_1, \cdots, x_n)$ の値はつねに正か 0 である．

（証明） $\tilde{k}$ の順序体としての拡大体で実閉体であるような $\tilde{K}$ をとる．$p(x_1, \cdots, x_n)$ がつねに正か 0 であるということは

$$\forall x_1, \cdots, x_n (p(x_1, \cdots, x_n) \geq 0)$$

と L_k の命題で書けてしかも K で成立しているから，前定理により，このことは $\tilde{K}$ でも成立している．$\tilde{k}$ は $\tilde{K}$ の順序体としての部分体であるから，$\tilde{k}$ でももちろん成立していなければならない．

つぎに代数学でよく知られた定理を借用することにする．いま体 k で -1 が平方の和で表わされないとき，すなわち k の任意有限個の元 $a_1, \cdots, a_n$ をとってきたとき

$$a_1^2 + \cdots + a_n^2 \neq -1$$

が成立するとき，k を**実体**であるという．実体は拡大して順序体さらに実閉体にすることができる．これを用いてつぎの補題を証明しよう．

補題 k は体で，k の元 a について，a は平方の和では表わされないとする．このとき $k(\sqrt{-a})$ は実体である．したがって順序を導入して，そこで $a<0$（すなわち $-a>0$）であるようにできる．

（証明） $k(\sqrt{-a})$ の任意の元は明らかにつぎの形である．

$$u + v\sqrt{-a}, \quad u, v \in k$$

万一，

$$\sum_i (u_i + v_i\sqrt{-a})^2 = -1$$

となったとすると

$$\sum_i u_i^2 - a\sum_i v_i^2 = -1$$

ゆえに

$$a = \frac{1 + \sum_i u_i^2}{\sum_i v_i^2} = \frac{(1 + \sum_i u_i^2)(\sum_i v_i^2)}{(\sum_i v_i^2)^2}$$

分子のカッコを開いてみれば，これは平方の和であることがただちにわか

り，分母も平方であるから，これは平方の和の形であり，a が平方の和で表わされないことに反する．

定理 17 いま k は実体で，k のいかなる元 a をとっても a か $-a$ かいずれか一方が必ず平方の和で表わされるものとする．いまさらに K は k の拡大順序体で実閉体であるとし，$p(x_1, \cdots, x_n) \in k[x_1, \cdots, x_n]$ が K のいかなる値に対してもつねに正か 0 をとるものとすれば，

$$r_1(x_1, \cdots, x_n), \cdots, r_m(x_1, \cdots, x_n) \in k(x_1, \cdots, x_n)$$

をとってつぎが成立するようにできる．

$$p(x_1, \cdots, x_n) = r_1^2(x_1, \cdots, x_n) + \cdots + r_m^2(x_1, \cdots, x_n)$$

（証明） k は実体であるから順序を入れることができるが，この順序の入れ方は一意的である．すなわち $a(\neq 0)$ が平方の和で表わされれば正，$-a$ が平方の和で表わされれば a を負とおくわけである．この定理の仮定と定理 16 の系とにより，k のいかなる拡大順序体においても $p(x_1, \cdots, x_n)$ は正または 0 の値しかとらないことがわかる．

さて $k(y_1, \cdots, y_n)$ において -1 は平方の和で表わされないことは明らかであるから，$k(y_1, \cdots, y_n)$ は k の拡大順序体であるとしてよい．したがっていかなる $k(y_1, \cdots, y_n)$ の拡大順序体をとっても $p(x_1, \cdots, x_n)$ は正の値または 0 をとる．

いま $p(y_1, \cdots, y_n)$ が $k(y_1, \cdots, y_n)$ で平方の和で表わされないとすると補題により $k(y_1, \cdots, y_n)$ の拡大順序体で $p(y_1, \cdots, y_n)$ が負であるようなものがある．これは矛盾する．（$p(y_1, \cdots, y_n)$ は $p(x_1, \cdots, x_n)$ の $x_1 = y_1, \cdots, x_n = y_n$ の値である．）

つぎの定理はヒルベルトの第 17 問題についてのアルティンの解答である．

定理 18 Q を有理数体として，

$$p(x_1, \cdots, x_n) \in Q[x_1, \cdots, x_n]$$

とする．Q のすべての値について $p(x_1, \cdots, x_n)$ が正または 0 をとるならば，$r_1, \cdots, r_m \in Q(x_1, \cdots, x_n)$ をとってつぎが成立するようにできる．

$$p(x_1, \cdots, x_n) = r_1{}^2(x_1, \cdots, x_n) + \cdots + r_m{}^2(x_1, \cdots, x_n)$$

（証明） R を実数体とすると R は実閉体である．さて $p(x_1, \cdots, x_n)$ は連続であるから，R のいかなる値に対しても $p(x_1, \cdots, x_n)$ はつねに正か 0 をとる．したがって前定理により，Q の任意の元 a に対して，a か $-a$ かが平方の和で表わされることを証明すれば十分である．ところで，m, n を正とすれば

$$\frac{n}{m} = \underbrace{\frac{1}{m^2} + \cdots + \frac{1}{m^2}}_{m \cdot n \text{ 個}}$$

であるから明らかである．

II　代数曲線へのロジックの応用

1.　ウルトラフィルター

いま X が集合であるとき，X の部分集合の族 F がフィルター (filter) であるということはつぎの条件をみたすことをいう．

1)　$X \in F$

2)　$A, B \in F \rightarrow (A \cap B) \in F$

3)　$A \in F, A \subseteq B \subseteq X \rightarrow B \in F$

4)　$\phi \notin F$

例をあげるならば，X の元 x をとったとき

$$F = \{A \subseteq X | x \in A\}$$

と F を定義するならば，F が X のフィルターになっていることは明らかである．

もう 1 つ例をあげると，N を自然数全体の集合，すなわち $N = \{0, 1, 2, 3, \cdots\}$ とするとき

$$F = \{A \subseteq N | N - A \text{ が有限集合}\}$$

とするとき，これがフィルターであることは容易に確められる．

F が X の上のフィルターであるとき，F が X の上のウルトラフィルターであることは，つぎの条件をみたすことをいう．

5)　$A \subseteq X \rightarrow A \in F \vee (X - A) \in F$

上にあげた 2 つのフィルターの例のうち，最初のフィルターは明らかにウルトラフィルターである．第 2 の例はウルトラフィルターではない．なぜならば

$$A_0 = \{0, 2, 4, \cdots\}$$

とおけば，　　　$A_0 \notin F, \quad (N - A_0) \notin F$

の 2 つが成立することは明らかである．

さて，F_α がフィルターの増大列すなわち

$$F_0 \subseteq F_1 \subseteq \cdots \subseteq F_\alpha \subseteq \cdots$$

であるとき
$$\bigcup_{\alpha} F_{\alpha}$$
を作れば，これもまたフィルターになることは明らかであるから Zorn の補題（または整列可能定理）を用いてつぎの定理は容易に証明される．

定理 1 F が X のフィルターであるとき，F を拡大したウルトラフィルター $\tilde{F}$ が必ず存在する．（すなわち $F \subseteq \tilde{F}$ であって $\tilde{F}$ はウルトラフィルター）

ここで注意すべきことは $\tilde{F}$ は一般には唯 1 通りには定まらないことである．注意し忘れたが，ウルトラフィルターを拡大することは不可能であることがただちにわかる．したがってウルトラフィルターはしばしば極大フィルターとも呼ばれる．

いまフィルターの第 2 の例にあげた F を定理 1 によってウルトラフィルターに拡大して，そうしてできたものの 1 つを F_0 としよう．（F のウルトラフィルターへの拡大の仕方は無数にある．）

この F_0 はつぎの著しい性質をもっている．
$$x \in X \rightarrow \{x\} \notin F_0 \wedge (X - \{x\}) \in F_0$$
この性質は F_0 のところへ F をおいても成立するから，F_0 の場合は明らかであるが，この性質が以下におもに用いられるものである．後々はおもにこのウルトラフィルターを用いるものとする．

2. ウルトラプロダクト

さて I を集合，F を I の上のウルトラフィルターとする．

いま 1 つの言語 L を固定する．L はつぎのごとくあたえられたとする．

変数：	$a, b, \cdots, x, y, z, \cdots$
特別な元を表わす記号：	$c_0, c_1, c_2, \cdots$
関数記号：	$f_0, f_1, f_2, \cdots$
predicate：	$=, P_1, P_2, \cdots$
論理記号：	$\neg, \wedge, \vee, \rightarrow, \forall, \exists$

いますべての I の元 i について，この言語についての数学的構造

$$\mathcal{S}_\iota=\langle S_\iota; c_0{}^\iota, c_1{}^\iota, \cdots, f_0{}^\iota, f_1{}^\iota, \cdots, P_1{}^\iota, P_2{}^\iota, \cdots\rangle$$

があたえられているとする．ここに S_ι は集合で $\mathcal{S}_\iota$ の universe または underlying set と呼ばれる．$c_j{}^\iota$ は S_ι の元であり，$f_j{}^\iota$ は S_ι の上に定義された（一般には多変数の）関数であり，もちろんその値は S_ι の元である．$P_j{}^\iota$ は S_ι の上に定義された predicate である（一般には多変数）ものとする．($P_1, P_2, \cdots$について $P_1{}^\iota, P_2{}^\iota, \cdots$ を考えながら，$=$ をのぞいたのは $=$ は $\mathcal{S}_\iota$ の上でも $=$ すなわち $a=b$ はやはり a と b とが同じものの意味に用いるからである．)

いま

$$\prod_{\iota\in I} S_\iota=\{g\,|\,(g: I \to \bigcup_{\iota\in I} S_\iota)\wedge\forall i\in I(g(i)\in S_\iota)\}$$

と定義する．すなわち $\prod_{\iota\in I} S_\iota$ は S_ι の集合としての直積である．

いま $g_1, g_2\in\prod_{\iota\in I} S_\iota$ のとき，

$$g_1\equiv g_2 \pmod{F}$$

を

$$\{i\in I\,|\,g_1(i)=g_2(i)\}\in F$$

によって定義しよう．

定理 2　$\equiv$ は $\prod_{\iota\in I} S_\iota$ の上の同値関係である．すなわちつぎの条件をみたす．

1)　$g\equiv g$

2)　$g_1\equiv g_2 \to g_2\equiv g_1$

3)　$g_1\equiv g_2, g_2\equiv g_3 \to g_1\equiv g_3$

(証明)　1)　は

$$I\in F$$

であり

$$I=\{i\in I\,|\,g(i)=g(i)\}$$

であるから明らか．

2)　は

$$\{i\in I\,|\,g_1(i)=g_2(i)\}=\{i\in I\,|\,g_2(i)=g_1(i)\}$$

であるから，明らか．

3)　は

$$A_1=\{i\in I\,|\,g_1(i)=g_2(i)\},\qquad A_2=\{i\in I\,|\,g_2(i)=g_3(i)\}$$

$$A=\{i\in I\,|\,g_1(i)=g_3(i)\}$$

とおけば，

$$A_1, A_2\in F$$

が仮定であり，証明したいことは $A \in F$ である．

ところで $\qquad i \in A_1 \cap A_2$

なる i をとれば $\qquad g_1(i)=g_2(i) \wedge g_2(i)=g_3(i)$

ゆえに $\qquad g_1(i)=g_3(i)$

ゆえに $\qquad i \in A$

このことから $\qquad A_1 \cap A_2 \subseteq A$

がわかる．ところで $A_1, A_2 \in F$ から

$$A_1 \cap A_2 \in F$$

がいえるから， $\qquad A \in F$

で証明が終った．

さて $\equiv$ は同等関係であるから， $\equiv$ で $\prod_{i \in I} S_i$ を類別することができる．この類別によってできる集合を

$$\prod_{i \in I} S_i / \equiv$$

と書くことにしよう．

くわしくいえば $\prod_{i \in I} S_i / \equiv$ の元は $g \in \prod_{i \in I} S_i$ なる g をとって

$$[g_0]=\{g \in \prod_{i \in I} S_i \mid g \equiv g_0\}$$

の形に書けるものである．このとき g_0 を $[g_0]$ の代表元という． 普通はよく， この類 $[g_0]$ とその代表元 g_0 とをあまりハッキリ区別しないで用いたりする．ただ代表元で議論するときは，いつでも代表元のとり方によらないということを証明したうえで， $\equiv$ をちょうど $=$ のような感じで用いるわけである．

さて $\mathcal{S}_i$ のウルトラプロダクトなる構造をつぎのごとく定義する．いま構成する構造を $\mathcal{S}$ と書くことにして

$$\mathcal{S}=\prod_{i \in I} \mathcal{S}_i / \equiv$$

または
$$\mathcal{S}=\prod_{i\in I}\mathcal{S}_i/F$$
と書くのが普通である．$\mathcal{S}$ は
$$\mathcal{S}=\langle S;\bar{c}_0,\bar{c}_1,\cdots,\bar{f}_0,\bar{f}_1,\cdots,\bar{P}_0,\bar{P}_1,\cdots\rangle$$
なる形をしていてこのそれぞれの $S,\bar{c}_0,\cdots$ を順々と定義していくことにする．S はいま定義した $\prod_{i\in I}S_i/\equiv$ であると定義する．

$\bar{c}_j$ はいま
$$g(i)=c_j^i$$
によって g を定義すれば
$$g\in\prod_{i\in I}S_i$$
となる，この g によって得られる類 $[g]$ によって $\bar{c}_j$ を定義する．

$\bar{P}_j$ はつぎのごとく定義する．まず P_j は言語 L で n 変数であるとする．このとき $[g_1],\cdots,[g_n]\in S$ について $\bar{P}_j([g_1],\cdots,[g_n])$ であることを
$$\{i\in I|P_j^i(g_1(i),\cdots,g_n(i))\}\in F$$
であることと定義する．ここでこの定義は代表元，$g_1,\cdots,g_n$ のとり方によらない．（これは簡単な演習問題であるから省略する．明らかでない人はぜひ自分で証明してその感じをつかんでほしい．）

最後に $\bar{f}_j$ はつぎのごとく定義する．いまやはり f_j は言語 L で n 変数の関数記号であるとして，$[g_1],\cdots,[g_n]\in S$ なる S の元を n 個とってくる．このとき $g\in\prod_{i\in I}S_i$ を
$$g(i)=f_j^i(g_1(i),\cdots,g_n(i))$$
と定義して
$$\bar{f}_j([g_1],\cdots,[g_n])=[g]$$
と定義するのである．このときもこの定義が代表元のとり方によらないことは容易に証明できる．

つぎの定理はウルトラプロダクトの基本定理といわれる．

定理 3
$$\mathcal{S}=\prod_{i\in I}\mathcal{S}_i/F$$
として，$A(a_1,\cdots,a_n)$ は言語 L のformula で，$a_1,\cdots,a_n$ だけが A のなかで自由変数として現われるものとする．このとき S から $[g_1],\cdots,[g_n]$ をとってくると

$$\text{‘}\mathcal{S}\text{ で }A([g_1],\cdots,[g_n])\text{ が成立する’}\leftrightarrow$$
$$\{i\in I\,|\,\mathcal{S}_i\text{ で }A(g_1(i),\cdots,g_n(i))\text{ が成立する}\}\in F$$

(証明) $A(a_1,\cdots,a_n)$ のなかの論理記号の数についての数学的帰納法で証明する.

1) 論理記号が 1 つもないとき

このときは $A(a_1,\cdots,a_n)$ は $P(t_1(a_1,\cdots,a_n),\cdots,t_m(a_1,\cdots,a_n))$ の形であり，ここに P は言語 L の predicate である.

$$\text{‘}\mathcal{S}\text{ で }P(t_1([g_1],\cdots,[g_n]),\cdots,t_m([g_1],\cdots,[g_n]))\text{ が成立する’}$$
$$\leftrightarrow\bar{P}(\bar{t}_1([g_1],\cdots,[g_n]),\cdots,\bar{t}_m([g_1],\cdots,[g_n]))$$

ここに $\bar{t}_j$ は t_j のなかの c や f を $\bar{c}$ や $\bar{f}$ にかえてできるものである. この同等は明らか.

$$\leftrightarrow\{i\in I\,|\,P^i(t_1{}^i(g_1(i),\cdots,g_n(i)),\cdots,t_n{}^i(g_1(i),\cdots,g_n(i)))\}\in F$$

ここに $t_j{}^i$ は t_j のなかの c や f を c^i や f^i にかえてできるものである. この同等は $\bar{P}$ の定義より明らか.

$$\leftrightarrow\{i\in I\,|\,P(t_1(g_1(i),\cdots,g_n(i)),\cdots,t_m(g_1(i),\cdots,g_n(i)))\text{ が }\mathcal{S}_i\text{ で成立する}\}\in F$$

2) $A(a_1,\cdots,a_n)$ が $\neg B(a_1,\cdots,a_n)$ の形のとき

$$\text{‘}\mathcal{S}\text{ で }A([g_1],\cdots,[g_n])\text{ が成立する’}$$
$$\leftrightarrow\ \neg(\mathcal{S}\text{ で }B([g_1],\cdots,[g_n])\text{ が成立する})$$
$$\leftrightarrow\ \neg(\{i\in I\,|\,B(g_1(i),\cdots,g_n(i))\text{ が }\mathcal{S}_i\text{ で成立する}\}\in F)$$
$$\leftrightarrow\ (I-\{i\in I\,|\,B(g_1(i),\cdots,g_n(i))\text{ が }\mathcal{S}_i\text{ で成立する}\})\in F$$

この同等は F がウルトラフィルターから得られる.

$$\leftrightarrow\{i\in I\,|\,B(g_1(i),\cdots,g_n(i))\text{ が }\mathcal{S}_i\text{ で成立しない}\}\in F$$
$$\leftrightarrow\{i\in I\,|\,\neg B(g_1(i),\cdots,g_n(i))\text{ が }\mathcal{S}_i\text{ で成立する}\}\in F$$

3) $A(a_1,\cdots,a_n)$ が $B(a_1,\cdots,a_n)\wedge C(a_1,\cdots,a_n)$ のとき $n=1$ として $A(a)$ について証明する.

$$X=\{i\in I\,|\,B(g(i))\text{ が }\mathcal{S}_i\text{ で成立する}\}$$
$$Y=\{i\in I\,|\,C(g(i))\text{ が }\mathcal{S}_i\text{ で成立する}\}$$

とおく.

$$\text{‘}\mathcal{S}\text{ で }A([g])\text{ が成立する’}$$

$$\leftrightarrow \text{‘}\mathcal{S}\text{ で }B([g])\text{ が成立する’} \wedge \text{‘}\mathcal{S}\text{ で }C([g])\text{ が成立する’}$$

$$\leftrightarrow X\in F \wedge Y\in F \qquad \text{(帰納法の仮定により)}$$

$$\leftrightarrow X\cap Y\in F \qquad (F\text{ はフィルターだから})$$

$$\leftrightarrow \{i\in I|\mathcal{S}_i\text{ で }B(g(i))\text{ と }C(g(i))\text{ とが成立する}\}\in F$$

$$\leftrightarrow \{i\in I|\mathcal{S}_i\text{ で }A(g(i))\text{ が成立する}\}\in F$$

4)　$A(a_1,\cdots,a_n)$ が $\exists xB(a_1,\cdots,a_n,x)$ のときやはり $n=1$ としてやる.

$$\text{‘}\mathcal{S}\text{ で }\exists xB([g],x)\text{ が成立する’}$$

$$\leftrightarrow \exists g'\in S(\mathcal{S}\text{ で }B([g],[g'])\text{ が成立する})$$

$$\leftrightarrow \exists g'\in S\{i\in I|\mathcal{S}_i\text{ で }B(g(i),g'(i))\text{ が成立する}\}\in F$$

これは帰納法の仮定からでる.

$$\rightarrow \{i\in I|\mathcal{S}_i\text{ で }\exists xB(g(i),x)\text{ が成立する}\}\in F$$

これは $B(g(i),g'(i))$ から $\exists xB(g(i),x)$ がでるから明らかである.

さて → だけしか証明しないから ← のほうもいわねばならない. いま

$$X=\{i\in I|\mathcal{S}_i\text{ で }\exists xB(g(i),x)\text{ が成立する}\}$$

とおくことにする.

$$X\in F$$

がいまわれわれの仮定である. いま $i\in X$

とすれば,

$$\text{‘}\mathcal{S}_i\text{ で }\exists xB(g(i),x)\text{ が成立する’}$$

がなりたつから, ある a_i が S_i に見つかって

$$\text{‘}\mathcal{S}_i\text{ で}B(g(i),a_i)\text{ が成立する’}$$

がなりたつようにできる. いま $g'\in\prod_{i\in I}S_i$ を

$$g'(i)=\begin{cases}a_i & i\in X\text{のとき}\\ \text{ある勝手な }S_i\text{ の元} & i\notin X\text{のとき}\end{cases}$$

によって定義する. このとき

$$\{i\in I|\mathcal{S}_i\text{ で }B(g(i),g'(i))\text{ が成立する}\}=X$$

は明らかであろう. ゆえに

$$\{i\in I|\mathcal{S}_i\text{ で }B(g(i),g'(i))\text{ が成立する}\}\in F$$

$$\rightarrow \text{‘}\mathcal{S}\text{ で }B([g],[g'])\text{ が成立する’}$$

$$\to\text{‘}\mathcal{S}\text{ で }\exists xB([g],x)\text{ が成立する’}$$

以上によって定理の証明は終った.

3. ウルトラパワー

いま I が集合で F は I のウルトラフィルターとする. 前節では $i\in I$ なるすべての i について数学的構造 $\mathcal{S}_i$ があたえられたと考えたが, こんどは唯 1 つの数学的構造 $\mathcal{T}$ だけがあたえられた場合を考えてみる. いますべての i について

$$\mathcal{S}_i=\mathcal{T}$$

だと思えば $\mathcal{S}_i$ がすべてあたえられたと考えられるわけである. このとき

$$\mathcal{S}=\prod_{i\in I}\mathcal{S}_i/F$$

によってできる構造を $\mathcal{T}$ のウルトラパワーといって

$$\mathcal{S}=(\mathcal{T})^I/F$$

によって表わす. この場合, 前の基本定理はただちにつぎの定理になる.

定理 4 $\mathcal{S}=(\mathcal{T})^I/F$

で $\mathcal{T}$ の underlying set を T とする.

いま $g_1,\cdots,g_n\in T^I$ であるとき

$$\text{‘}\mathcal{S}\text{ で }A([g_1],\cdots,[g_n])\text{ が成立する’}$$
$$\leftrightarrow\{i\in I\mid\mathcal{T}\text{ で }A(g_1(i),\cdots,g_n(i))\text{ が成立する}\}\in F$$

この定理からただちにつぎの系がでる.

系 $\mathcal{S}=(\mathcal{T})^I/F$

で, A は言語 L の命題であるとする. そのとき

$$\text{‘}\mathcal{S}\text{ で }A\text{ が成立する’}\leftrightarrow\text{‘}\mathcal{T}\text{ で }A\text{ が成立する’}$$

すなわち, $\mathcal{S}$ と $\mathcal{T}$ とは命題が成立するという点に関してはまったく同じようにふるまうことがわかる.

以下われわれはウルトラパワーについてだけ考えることとする.

さて
$$\mathcal{S}=(\mathcal{T})^I/F$$
とするとき，いま $\mathcal{T}$ を $\mathcal{S}$ の部分構造と考えられることをいおう．

$a\in T$ なる元 a について，$g_a\in T^I$ を

$$\text{すべての } i\in I \text{ について } g_a(i)=a$$

によって定義すれば明らかに

$$\begin{array}{ccc} \mathcal{T} & & \mathcal{S} \\ b=f(a_1,\cdots,a_n) & \leftrightarrow & g_b=f(g_{a_1},\cdots,g_{a_n}) \\ P(a_1,\cdots,a_n) & \leftrightarrow & P(g_{a_1},\cdots,g_{a_n}) \end{array}$$

となることは明らかであるから，$\mathcal{T}$ は $\mathcal{S}$ に同型に入れこむことができる．ゆえに今後 $\mathcal{T}$ は $\mathcal{S}$ の部分構造と考える．この g_a と書いたものはしばしば a 自身によって表わされる．

4.　N のウルトラパワー

前にのべたように N は自然数全体の集合である．以下に F_0 は第 1 節でのべた N の上のウルトラフィルターとして，以下この F_0 のみを考えることにする．

いま N は $0,1,2,\cdots$, $+$, $\cdot$ や $<$ などの自然数を表わす記号，関数や predicate をもっているものとする．その他必要なものは必要なだけ考えることにする．

ここで考えるのは N^N/F_0 であるが，これを単に
$$*N$$
と書くことにする．$*N$ の元は $f\in N^N$ なる関数によって代表される．

最初に $*N$ のなかの $0,1,2,\cdots$ は前節の定義によって，その値がそれぞれ $0,1,2,\cdots$になるようなコンスタントな関数であることを注意してほしい．いま
$$g(i)=i$$
によって $g\in N^N$ を定義すると，$n\in N$ なる n について
$$n<g$$

$$\leftrightarrow \{i \mid n < g(i)\} \in F_0$$

$$\leftrightarrow (N - \{0, 1, 2, \cdots, n\}) \in F_0$$

ところで最後の式は F_0 の定義によりつねに成立しているから

$$\forall n \in N (n < g)$$

がいえることがわかる．すなわち $^*N$ は N とまったく同じ命題をみたすが N 以外の元があることがわかる．いま N の元 n をとってきて $g \in {}^*N$ なる元について

$$g \leq n$$

が成立していたとする．

ところで N は

$$\forall x (x \leq n \rightarrow x = 0 \vee x = 1 \vee \cdots \vee x = n)$$

をみたす．$^*N$ は N と同じ命題をみたすから，この命題は $^*N$ でも成立している．$g \in {}^*N$ であるから

$$g \leq n \rightarrow g = 0 \vee g = 1 \vee \cdots \vee g = n$$

となって

$$g \in N$$

であることがわかる．すなわち $^*N$ の N 以外の元は，すべての N の元より大きいということがわかる．したがって $^*N - N$ の元をわれわれは無限大と呼ぶのである．

いま

$$g \in {}^*N - N$$

とする．N において

$$\forall x (x < x + 1)$$

は成立しているから，これは $^*N$ でも成立している．$g \in {}^*N$ であるから，特別の場合として

$$g < g + 1$$

がでてくる．g も $g+1$ も無限大であるが，相異なる無限大であるわけである．いったい $g+1$ はどんな関数になっているのであろうか？

$$(g+1)(i) = g(i) + 1$$

とおけばよいことは，簡単にわかるから証明してみていただきたい．

同様にして

$$\forall x (1 < x \rightarrow x < 2 \cdot x)$$

は N で，したがって $^*N$ で成立するから，無限大の g に対しては

$$g<2\cdot g$$

が成立する．ここで前と同じように $2\cdot g$ はどんな関数によって表わされるかを調べてみると

$$(2\cdot g)(i)=2g(i)$$

とおけばよいことが容易にわかる．

このように $^*N$ について無限大が入っていても N と同じように計算することができる．この $^*N$ が数学的帰納法の公理をみたしているということはちょっと不思議な気がするが，じつはこの数学的帰納法の公理はわれわれの言語 L のなかで表現できるものだけにかぎるのである．

もう少しくわしく説明するとつぎのようになる．N の任意の部分集合を表わす predicate を全部われわれの言語 L のなかに入れておいてもさしつかえない．すなわち N の任意の部分集合がわれわれの言語のなかで表わされるようにしておく．こうしたうえで $^*N$ をとるとどうなるか？ N の部分集合 S について $^*S$（これは $^*N$ のなかで同じ文字 S が表わすもの）なる $^*N$ の部分集合が作られる．この $^*S$ について最小な数の存在が $^*N$ でいえる．しかしながら $^*N$ の任意の部分集合はこのように最も一般にわれわれの言語を拡張しておいても表わすことができないのである．すなわち $^*N$ には無限大があるから $^*N$ の外部から $^*N$ をながめると最小原理が成立しないような $^*N$ の部分集合 M が存在するのであるがこの M は N の部分集合 S をとって $^*S$ なる形では絶対表わせないのである．この間の事情はいろいろとこの $^*N$ でゲームを遊んでみて実際に痛感していただきたい．

これは大切なことであるから，さらに本質的な点について説明してみたい．いま N だけを考えずに N の集合全部またはその N の集合の集合を全部というふうにいくらでもつけ加えて考えることができる．

きちんと表現するには $\mathcal{T}=\langle T,\cdots\rangle$
のなかに $\in$ という predicate を入れておき N の元も，N の集合も，N の集合の集合も，… もすべて T の元であると考えるのである．こうして

$$\mathcal{S}=(\mathcal{T})^N/F_0$$

を考えると $\mathcal{S}$ のなかで $*N$ および $*N$ の集合にあたるもの，$*N$の集合の集合にあたるもの，… がでてくるわけである．

このとき $\mathcal{T}$ において N のすべての集合について，最小値存在が成立するから，$\mathcal{S}$ においても $*N$ のすべての集合について，最小値存在が成立するのである．

ここで大切なのは，'$\mathcal{S}$ **においても**' ということである．$*N$ の任意の部分集合をとればもちろん最小値存在がいえないものがあるわけであるが，$\mathcal{S}$ という構造のなかで $*N$ の集合であるとして認められたものについては，たしかに最小値の存在がいえるのである．別ないい方をすればウルトラパワーという構成により作られた $*N$ の部分集合については，最小値の原理が成立しているわけである．したがって以下において，$\mathcal{S}$ のなかの $*N$ の部分集合（またはウルトラパワーによって作られた$*N$の部分集合）という概念を一般の（$\mathcal{S}$ の外からながめたときの）集合と区別することが大切になる．この $\mathcal{S}$ の内部（またはウルトラパワーによって構成されたとき）の概念のとき internal といい，$\mathcal{S}$ の外からながめた一般の概念のとき external というのである．すなわち internal な $*N$ の集合，internal な $*N$ から $*N$ への関数というふうに用いる．N と $*N$ とはもし $*N$ の internal な概念だけを用いて考えているぶんにはまったく同じ命題が成立するのであるが，一度 $*N$ の external な概念をもちだせばまったく異なった現象が生じてしまう．このことがあとでいろいろな議論をするときに大切なことである．すなわちわれわれは internal な概念と external な概念との関係を調べることによっていろいろと新しい結果を得ようというのである．

この external ということにもうちょっと注意を加えると，もともとの$\mathcal{T}$についての概念の多くが $\mathcal{S}$ では external な概念となる．たとえば上の N は $\mathcal{S}$ では external な概念である．なぜならばもし N が $\mathcal{S}$ で internal な概念であれば $*N-N$ も $\mathcal{S}$ で internal，したがって $\mathcal{S}$ の最小性の原理により $*N-N$ の最小値 ω が存在しなければならない．ところで $\omega\neq0$（実際には無限大）であるから $*N$ で成立するペアノの公理によって

$$(\omega-1)\in{}^*N\wedge(\omega-1)<\omega$$

となり，一方もし　$(\omega-1)\in N$

ならば $\omega\in N$ となるから　$\omega\notin N$

も明らかであり，これは ω の最小性に矛盾する．

5.　実数のウルトラパワー

R を実数全体の集合として，R^N/F_0 を考える．この構造を $^*R$ と書くことにする．もちろんわれわれの言語 L には，すべての実数から実数への関数，すべての実数についての predicate を表現できるように十分豊富にとっておくのである．

まず $^*N$ の場合と同じように

$$g(i)=i \qquad \text{すべての } i\in N \text{ について}$$

と定義すればすべての実数 r について

$$r<g$$

であることが容易にいえる．すなわちこの g は前と同じく正の無限大である．この正の無限大に $-$ をつけて考えれば

$$\forall x,y\,(x<y \rightarrow -y<-x)$$

は R でしたがって $^*R$ で成立しているから，特別の場合として

$$r<g \rightarrow -g<-r$$

が得られ，$-g$ はすべての R の元より小さい元，すなわち負の無限大であることがわかる．

いままた，g を正の無限大，すなわち

$$\forall r\in R(r<g)$$

が成立する $^*R$ の元であるとする．

$$\forall x,y\left(0<x<y \rightarrow 0<\frac{1}{y}<\frac{1}{x}\right)$$

は R で成立，したがって $^*R$ で成立するから，特別な場合としてわれわれは

$$0<\frac{1}{g}<\frac{1}{r}$$

がすべての正な R の元 r に対して成立することがわかる．すなわち $\dfrac{1}{g}$ は正の無限小であることがわかる．同様にして負の無限小の存在もわかる．

さていま，$g\in{}^*R$ を正の無限大でもなく，負の無限大でもないとしよう．すなわち

$$\exists r, s\in R(r<g<s)$$

が成立しているものとする．

このとき $$\{x\in R \mid x<g\}$$

を考えると，これは実数のデデキントの切断を構成することは明らかであろう． この切断によって定義される実数を r_0 とおこう． いま $g-r_0$ が無限小，すなわち $|g-r_0|$ が 0 か正の無限小であることを証明しよう．

いまもし正の実数 ε があって

$$\varepsilon\leq|g-r_0|$$

であったとする．$g\leq r_0-\varepsilon$ の場合と $r_0+\varepsilon\leq g$ の場合とがあるが，いずれも

r_0 の定義に反する

ことは明らかであろう．

以上によって，${}^*R$ の元 g は

1) 正の無限大

2) 負の無限大

3) ある実数 r_0 があって $g-r_0$ が無限小

と 3 つの場合に分けられることがわかる．この第 3 の場合にわれわれは g が有限であるということとする．この場合，$g-r_0$ なる r_0 が唯 1 通りに定まることは明らかであるからこの r_0 のことを

$${}^0(g)$$

と書くことにする．

少し例を考えることにすれば

$$g(i)=1/i \qquad \text{すべての } i\in N \text{ について}$$

と定義すれば g は正の無限小となり，

$${}^0(g)=0$$

となる．

$$g_1(i)=i \qquad \text{すべての } i\in N \text{ について}$$

$$g_2(i)=i^2 \qquad \text{すべての } i\in N \text{ について}$$

と定義すれば g_1 も g_2 もともに無限大であるか，

$$g_1<g_2 \wedge g_2=(g_1)^2$$

が成立する．g_1+g_2 なる関数はつぎのものによって表わされる．

$$(g_1+g_2)(i)=i^2+i$$

N は R の部分集合であるから，N をわれわれの言語 L のなかに入れておいてもよい．すなわち　$N(x)$
あるいはこれを $x\in N$ と書いて，'x は自然数である' と読むのである．このとき実数はアルキメデスの公理をみたす．すなわち

$$\forall x \exists n (N(n) \wedge x<n)$$

をみたす．したがって，これは $^*R$ でみたされる．このことは，$^*R$ に無限大の元があるから変であるように思われるが，じつは $^*R$ でこの性質が成立するということを吟味してみると $^*R$ で $N(g)$ が成立するということは，

$$\{i\in N \mid N(g(i))\}\in F_0$$

ということなのである．すなわち $g\in {}^*N$ ということを意味するのである．すなわち上の式が $^*R$ で成立することは

$$\forall x \exists n\in {}^*N (x<n)$$

を意味し，$^*N$ のなかにも無限大があるから別に矛盾が生ずるわけではない．

同じように有理数全体は R の部分集合であるから，有理数の集合 Q というのをわれわれの言語 L にくり入れておいてもよい．R は

$$\forall x \forall y (x<y \rightarrow \exists z\in Q (x<z<y))$$

なる命題をみたす．したがってこれは $^*R$ でも成立する．これは 2 つの正の無限小をとれば，その間に有理数は 1 つもないから矛盾するようにみえるが，前と同じく，上の意味を吟味してみれば，これは

$$\forall x \forall y (x<y \rightarrow \exists z\in {}^*Q (x<z<y))$$

であってこの $^*Q$ のなかには無限小のものも入っているのである．

よく知られたように N と Q とは 1 対 1 の対応がある．この 1 対 1 の対応の 1 つを f として，この f に相当するものをわれわれの言語 L のなかに入れておくことができる（f に相当するものといったのは，f を N に制限したとき 1 対 1 になる関数か，または集合の形で入れておくという意味である）．そうすると

'f は N と Q との 1 対 1 の対応である'

はわれわれの言語で書くことができて R で成立している．したがってこれは $^*R$ でも成立している．しかしその意味は

'$^*f$ は $^*N$ と $^*Q$ との 1 対 1 の対応である'

ということになるのである．

以上によってだいたいの感じはわかったことと思う．つぎに本論に入っていくことにする．

6. 代数体のウルトラパワー

さて k を代数体として，k はある特定な仕方で複素数全体の体 C のなかに入っているものとする．すなわち k は C の部分体と考える．

前と同じように $(k)^N/F_0$ を考えるのであるが，実際にはもっと大きく，$(C)^N/F_0$ を作ることにする．しかも言語 L をできるだけ大きくとっておいて，C の部分集合とか，C の上の多変数の関数など全部入るようにしておく．いまのところ必要かどうかわからないが，必要ならば C の集合の集合というようなものも入れておいて一向にさしつかえない．したがって k の部分体とか，ある整域でのイデアルとかいつでも論ずることができる．

とにかくこうしてウルトラパワーで k からできたものを $^*k$, C からできたものを $^*C$ と書くことにしよう．k と $^*k$ とは同じ公理をみたすから $^*k$ ももちろん標数 0 の体である．

いま $f(x,y)$ を $k[x,y]$ の既約多項式として，$f(x,y)=0$ の作る既約な代数曲線を Γ とおくことにする．$^*\Gamma$ がちょうど $f(x,y)=0$ が作る $^*C$ での代数曲線で代数幾何では同じ Γ を用いて表わすのが慣用である．（した

がって以下でもそのようにする.)

$^*k$ の元で k の元でないものを $^*k$ の nonstandard な元といい，k の元になるのを standard な元というふうにいう．nonstandard な複素数といえば $^*C-C$ の元であり，standard な複素数といえば C の元を意味する．同じように，Γ の nonstandard な点といえば，じつは $^*\Gamma$ と Γ とを区別したときの $^*\Gamma-\Gamma$ の点のことをいい，Γ の standard な点というのはもともと Γ に属する点をいうのである．

ちょっと脱線してしまったが，先にのべたような既約な多項式 $f(x, y)$ によってできる代数曲線 Γ を考えることにする．いま点 (ξ, η) が Γ の generic point であるということを，$g(x, y) \in k[x, y]$ なる任意の多項式 g をとったとき $g(\xi, \eta)=0$ ならば Γ の任意の点において g が 0 となることと定義しよう．

いま点 $A=(\xi, \eta)$ が Γ の nonstandard な点とする．すなわち $f(\xi, \eta)=0$ で ξ と η の少なくとも一方は standard ではない． このとき A は Γ の generic point になる．

これを証明するために任意の $g(x, y) \in k[x, y]$ をとってきて，$g(\xi, \eta)=0$ で g は Γ の上で恒等的には 0 にならないとする．そうすると $f(\xi, \eta)=0$ と $g(\xi, \eta)=0$ とは互いに独立であるからこの 2 つの方程式から ξ と η とを代数的に解くことができ，ξ と η とは代数的数になり，したがって C の元であり，nonstandard なものが少なくとも 1 つあるということに反することになる．

つぎに Γ が座標が k の元だけからなる点を無限にもっていたとしよう．このときにこれらの点を全部くり返しなしに並べて $A_0, A_1, A_2, \cdots$ とすることができる．くわしくいえばこれは N から $k \times k$ への関数であるが，このような関数ははじめからわれわれの言語 L のなかに入っているものと思ってよい．

いま無限大の自然数の 1 つをとってきてこれを ω と書くことにする（すなわち ω は nonstandard な自然数である)．われわれのウルトラパワーに

おいては A_ω が定義できて，

$$A_\omega \in {}^*k \times {}^*k \quad \text{で} \quad A_\omega \in \Gamma$$

であることは明らかである．いま A_ω が standard な点でないことをいおう．もし A_ω が standard な点であるとすると，有限の自然数 n をとってきて

$$A_n = A_\omega$$

なるような n が存在する．ところで $A_0, A_1, \cdots$ はくり返しがないようにとったのであるから，

$$\forall n, m(n \neq m \rightarrow A_n \neq A_m)$$

がもともと成立しており，したがってわれわれのウルトラパワーでも成立しているから $\qquad A_n \neq A_\omega$

がいえて矛盾する．いま A_ω は nonstandard であることがわかったから A_ω は Γ の generic point になっている．

いま逆に Γ が ${}^*k \times {}^*k$ の点 A を generic point としてもっているとする．このとき $A = (\xi, \eta)$ とすると，ξ, η が双方とも代数的数でありえない．(もしそうだと ξ と η が満足する多項式をそれぞれ，$g(x)=0, h(y)=0$ とおくと，$f(x, y)=0 \rightarrow g(x)\cdot h(y)=0$ となり f の既約性に反する．）したがって A は nonstandard な点になっている．このことから Γ には $k \times k$ の点が無限に存在することが証明される．なぜならば，いま Γ の上の $k \times k$ の点 $A_1, \cdots, A_n$ をとってきたとき ($n=0$ のときも入れて)

$$A \neq A_0 \wedge \cdots \wedge A \neq A_n$$

であるから

$$\exists x \in \Gamma (x \neq A_0 \wedge \cdots \wedge x \neq A_n)$$

はわれわれのウルトラパワーで成立している．したがってわれわれのもともとの代数体でも成立している．これは $k \times k$ の Γ の点が少なくとももう1個存在することを意味している．

7. 体の valuation

少しばかり代数学のおさらいをすることにする．

K が体で，P が順序体であるとする．このとき $v:K \to P$ なる関数が K の valuation であるということは，つぎの 3 つの条件をみたすことをいう．

1)　$a \neq 0$ ならば $v(a) > 0$ で $v(0)=0$

2)　$v(a \cdot b) = v(a) \cdot v(b)$

3)　$v(a+b) \leq v(a) + v(b)$

だいたいに思って絶対値 $|a|$ を公理化したものと思えばよい．ただちにでてくる簡単な性質として

$$v(1) = v(-1) = 1$$

$$v(a) = v(-a)$$

$$|v(b) - v(a)| \leq v(b-a)$$

などがある．

いまもし $\mathfrak{o}$ が整域であって，K がその商体であるとし，$\mathfrak{p}$ を $\mathfrak{o}$ の素イデアルとするとき，$a \in \mathfrak{o}$ に対して，n を，

$\mathfrak{p}^n$ は a を割るが，$\mathfrak{p}^{n+1}$ は a を割らない数

と定義し，

$$v(a) = e^{-n} \qquad a \neq 0 \text{ ならば}$$

$$v(0) = 0$$

と定義すれば，多くの $\mathfrak{o}$ に対して v は上の 1), 2), 3) の条件をみたす．このとき，さらに K の元 a に対しては $a = b/c$, $b, c \in \mathfrak{o}$ となるような $\mathfrak{o}$ の元を見出して

$$v(a) = \frac{v(b)}{v(c)}$$

と定義すればよい．この v の定義が b, c のとり方によらないこと，およびこの v が 1), 2), 3) の条件をみたすことはほとんど明らかであろう．このvaluation は $\mathfrak{p}$-adic と呼ばれ $v_{\mathfrak{p}}$ と表わされる．

とくに $\mathfrak{o}$ で因数分解が一意的にできるとき $\mathfrak{p}$ が $\mathfrak{o}$ の素数 p からできる素主イデアル (p) のときは $v_{\mathfrak{p}}$ は明らかに上の 1), 2), 3) の条件をみたし，このとき，$v_{\mathfrak{p}}$ を p-adic valuation といって v_p と書く．

つぎに P がアルキメディアン順序体であるときは，P は実数体の部分体

であると思ってよいから，v の値は実数であると思ってさしつかえない．いまこのような値が実数であるような valuation v について，v がアルキメディアンでないということを

どんな $n=1+1+\cdots+1$ をとってきても，$\varphi(n)\leq 1$ が成立すること

と定義する．上にのべた $\mathfrak{p}$ でできる $v_{\mathfrak{p}}$ はアルキメディアンでない valuation である．このことは P がアルキメディアンということとは何の関係もないから注意すべきである．

v がアルキメディアンでない必要十分条件は 3) の代りにつぎの 3′) をみたすことであることが知られている．

3′) $$v(a+b)\leq \max(v(a), v(b))$$

したがってアルキメディアンでない valuation をはじめから 3′) で定義することが多い．

いい忘れたが，valuation のなかで

$$v(a)=1 \qquad a\neq 0 \text{ のとき}$$
$$v(0)=0$$

によって定義されるものをトリビアルな valuation という．

valuation v があたえられたとき，もし v の値が実数であるときには $a, b \in K$ なる a, b 間の距離を $v(a-b)$ であたえればこれは距離空間になることは容易にわかる．したがって v は K に 1 つの位相をあたえることになる．v の値が実数でないときでも，同じような考えで近傍を定義して位相空間を作ることは容易にできる．(一様位相)．いずれにしても v によってあたえられる位相空間がわれわれにとっては大切なのである．(上のトリビアルな valuation からは discrete な位相があたえられる．) 2 つの valuation が同じ位相をあたえるとき，この 2 つの valuation を equivalent といってだいたい同じ valuation だと思うのである．もし valuation の値が実数とかぎっておけば，2 つのトリビアルでない valuation v_1, v_2 が互いに equivalent である必要十分条件は $\lambda>0$ なる実数 λ が存在して

$$v_1(a)=(v_2(a))^{\lambda}$$

がすべての $a \in K$ について成立することである．

K にアルキメディアン valuation があると K は複素数体の部分体であって，その valuation は複素数の絶対値 $|\ \ |$ のあたえる valuation だと思ってよいことがわかっているから，アルキメディアン valuation は本質的にはあまり興味がない．それで valuation といえば単にアルキメディアンでない valuation だけのことを意味することも多い．したがって 3) の定義の代りに最初から 3′) を valuation の定義としてとることも多い．

いまこの場合（すなわちアルキメディアンでない場合で 3′) を基本的な定義としてとる場合）を考えてみると P が体である条件は必要がないことがすぐわかる．すなわち 1)，2)，3′) には P の元の加法はどこにも用いられていない．だから P の負でない元を乗法に関してだけとりあげることができればよいわけである．いま P の正のところだけを考えて Π とすれば Π は乗法に関して群になっている．

$$S=\{a \in P \mid 0 < a < 1\}$$

とすると

$$\Pi = S \cup \{1\} \cup S^{-1}$$

の形に書ける．S は半群になっていることは明らかであるから，この場合に理論を構成しようと思えば

1) Π は乗法についての可換群

2) $\Pi = S \cup \{1\} \cup S^{-1}$ は直和である．

3) S は半群である．

4) $a, b \in \Pi$ について $a < b$ を $ab^{-1} \in S$ によって定義する．したがって $a < 1 \leftrightarrow a \in S$.

以上を Π について必要な性質とすればよい．この上でアルキメディアンでない valuation の定義をするためには Π に新しい元 0 をつけ加えて，Π のすべての元 a について

$$0 \cdot a = 0 \quad \text{で} \quad 0 < a$$

という性質をつけ加えておけばよい．こうしておけば，アルキメディアンでない valuation をより一般に定義することができる．

以下にわれわれは代数体の valuation について考えることが多いので，代数体の valuation についてのつぎの定理を証明なしでのべておく．

定理 5 代数体 K のすべてのアルキメディアン valuation は K をすべての可能な方法で複素数体に入れこみ，そして

$$v(a)=|a|^{\lambda}, \quad 0<\lambda\leq 1$$

とおくことによって得られる．すなわち equivalent な valuation をのぞいては

$$v(a)=|a|$$

だけだと思ってよい．（うめこみ方を決めたうえで）

つぎに K のすべてのアルキメディアンでない valuation は equivalent なものをのぞいては K の素イデアル $\mathfrak{p}$ からできる $\mathfrak{p}$-adic valuation $v_{\mathfrak{p}}$ になっている．

この定理から明らかなことは，K を複素数体にうめこむ仕方は有限個しかないから K のアルキメディアンな valuation は有限個しかないということである．K の素イデアルは無限にあるから K のアルキメディアンでない valuation は無数にある．

つぎに valuation と密接な関係にある place についてのべることにしよう．

いま F は体であるとする．いま F に ∞ なる新しい要素をつけ加えて，F の元と ∞ との間の代数計算をつぎのように行なうこととする．

$$a\pm\infty=\infty, \quad a\cdot\infty=\infty \ (a\neq 0 \text{ とする}),$$

$$\infty\cdot\infty=\infty, \quad 1/0=\infty, \quad 1/\infty=0.$$

$\infty\pm\infty, 0\cdot\infty, 0/0, \infty/\infty$ は定義がされていないものとする．

φ が K から F の place であるというのは φ が

$$\varphi: K \to F\cup\{\infty\}$$

なる準同型写像（$+$ と $\cdot$ についての）であって

$$\varphi(1)=1$$

なる条件をみたしていることをいう．ここで準同型という意味は ∞ や 0 が

入ってくるときは準同型の条件は上にのべたような計算ができるときだけ成立することを要求するものである.

このとき，φ は単に F-valued といわれる.

$$\varphi(a)\neq\infty$$

であるような K の元 a をこの place で有限であると呼ぶ.

$$\mathfrak{o}=\{a\in K\mid\varphi(a)\neq\infty\}$$

と $\mathfrak{o}$ を定義すると $\mathfrak{o}$ は明らかに環である.（以下環はつねに可換で，零因子はなく，1 があるものとする.）さらに

$$\varphi(a)\neq 0, \infty$$

ならば

$$a^{-1}\in\mathfrak{o}$$

となるから $\mathfrak{o}$ の φ による像は体となる. 以下においてわれわれはつねにこの φ による $\mathfrak{o}$ の像が F 自身，すなわち φ は onto な写像であると考えることにする.（必要ならば名前をかえればよいだけだから).

$$\mathfrak{p}=\{a\in\mathfrak{o}\mid\varphi(a)=0\}$$

とおけば $\mathfrak{p}$ は明らかに極大イデアルで

$$\mathfrak{o}/\mathfrak{p}\simeq F$$

となる.

この $\mathfrak{o}$ はつぎの性質をみたす.

$$a\in K, a\notin\mathfrak{o} \;\rightarrow\; a^{-1}\in\mathfrak{o}$$

一般に体 K の部分環 $\mathfrak{o}$ がこの条件をみたしたときに，$\mathfrak{o}$ のことを valuation 環，つづめて v-環と呼ぶことにする.

K が体で $\mathfrak{o}$ がその v-環であったとする. このとき $\mathfrak{o}$ の unit でない元の全体を $\mathfrak{p}$ とすると，$\mathfrak{p}$ は極大イデアルになっている.

これを証明するために，$a\in\mathfrak{p}$, $c\in\mathfrak{o}$ とすれば明らかに ca は unit ではなく，したがって $\mathfrak{p}$ の元である. つぎに $a, b\in\mathfrak{p}$ とすれば，$\mathfrak{o}$ が v-環であるから，a/b か b/a のいずれかが $\mathfrak{o}$ の元となる. 一般性を失わないから $a/b\in\mathfrak{o}$ とする. ゆえに，$1+a/b=(a+b)/b\in\mathfrak{o}$. いま $a+b$ が $\mathfrak{p}$ の元でないとすると，$1/a+b\in\mathfrak{o}$ したがって $1/b\in\mathfrak{o}$ となり，b が unit でないことに反する.

$\mathfrak{p}$ が極大であることは $\mathfrak{p}$ に入らない $\mathfrak{o}$ の元が unit であることから明らかである．

いま
$$\mathfrak{o}/\mathfrak{p}=F$$
とおけば F は体となる．

いま
$$\varphi: K \to F\cup\{\infty\}$$
を
$$a\in\mathfrak{o} \text{ ならば } \varphi(a)=a/\mathfrak{p}\in F$$
$$a\notin\mathfrak{o} \text{ ならば } \varphi(a)=\infty$$
と定義すれば，φ は place であることは明らかであろう．

いま 2 つの place
$$\varphi_1: K\to F_1,\qquad \varphi_2: K\to F_2$$
(φ_1,φ_2 は onto であるとする）があったとき，φ_1,φ_2 が equivalent であるということを
$$\lambda: F_1 \to F_2$$
なる同型写像があって
$$\varphi_2=\lambda\varphi_1 \quad (\lambda(\infty)=\infty \text{ とする})$$
が成立することとして，
$$\varphi_1\sim\varphi_2$$
で表わす．

$\varphi_1\sim\varphi_2$ のための必要十分条件は φ_1,φ_2 が同じ v-環をもつことであることは明らかであろう．

さて，valuation と place の関係についてのべよう．

φ が K の place で，その v-環を $\mathfrak{o}$，極大イデアルを $\mathfrak{p}$, $\mathfrak{o}$ の unit の集合を U としよう．このとき
$$K^\times=K-\{0\},\qquad \mathfrak{p}^\times=\mathfrak{p}-\{0\}$$
とすると
$$K^\times=\mathfrak{p}^\times\cup U\cup\mathfrak{p}^{\times-1} \qquad (\text{直和})$$
が成立し，$K^\times$ は乗法に関して群になっており U は部分群になっている．

因子群 $K^\times/U$ を作って

$$v : K^{\times} \to K^{\times}/U$$

なる準同型写像 v を表わすこととして，さらに

$$v(0)=0$$

によって v を定義すれば

$$\Pi=K^{\times}/U, \qquad S=\mathfrak{p}^{\times}/U$$

と定義したうえで v が valuation になることは明らかであろう．

逆に valuation v が

$$v : K \to \Pi \cup \{0\}$$

によってあたえられているとする．このとき

$$\mathfrak{o}=\{a \in K \mid v(a) \leq 1\}$$

とすれば $\mathfrak{o}$ は v-環になり，

$$v(a)=1$$

が a が $\mathfrak{o}$ の unit の必要十分条件となる．したがって極大イデアル $\mathfrak{p}$ は

$$\{a \in v \mid v(a) < 1\}$$

となる．

アルキメディアンでない valuation のときはしばしば別の記号法が用いられる．いま v の値が実数として

$$w(a)=-\log v(a)$$

とおけば

1)　$a \neq 0$ ならば $w(a)$ は実数である

2)　$w(0)$ は ∞ とおく

3)　$w(ab)=w(a)+w(b)$

4)　$w(a+b) \geq \min(w(a), w(b))$

この場合のほうが便利なのは，たとえば素イデアル $\mathfrak{P}$ からできる valuation の場合は

$w_{\mathfrak{P}}(a)$ はちょうど $\mathfrak{P}$ の何乗が a を割るかになっている

というようにキレイに表現される．

したがってわれわれも次節からこの $w_{\mathfrak{P}}$ のほうの記号法をとることにし

て，ここに書いた $w_{\mathfrak{P}}$ を単に $v_{\mathfrak{P}}$ と書くことにする．このときその値の群は加法群でありしかも 0 の代りに ∞ が入っていることに注意すべきである．

8. internal valuation

代数体 k のウルトラパワー $^*k$ の internal valuation を考えることにする．ここで internal の意味は前にのべたように k の部分集合をすべてわれわれのもともとの構造（これをやはり $\mathcal{T}$ と書く）のなかに含めておいて，この構造のウルトラパワーによってできる構造（これをやはり $\mathcal{S}$ とする）のなかに表われる $^*k$ の集合のことを internal な集合という．同じように k から実数への関数もすべてわれわれの構造のなかに含めておけば，この構造のウルトラパワーのなかには $^*k$ から $^*R$へ の関数になるものもたくさん入ってくる．このようにわれわれのウルトラパワーのなかに入っている $^*k$ から $^*R$ への関数をやはり internal というのである．(われわれのウルトラパワーのなかに入っていない一般の集合や関数のことを一般に external という.）さて valuation は関数（または写像といってもよい）の特別なものであるから，internal valuation というのは $^*k$ の valuation でわれわれのウルトラパワーのなかに入っているものといってよい．

さて $^*k$ の internal valuation はどのようなものであろうか？

まず k は代数体であるから，$^*k$ はわれわれのウルトラパワーのなかでは $^*Q$ の上の代数体である（Q を有理数体とするとき，$^*k$ のウルトラパワーのなかの基礎体は $^*Q$ であって Q ではない)．したがって定理 5 により $^*k$ の internal valuation はアルキメディアン valuation か $^*k$ の素イデアルからできるアルキメディアンでない valuation かどちらかである．

まず $^*k$ の素イデアルからできる valuation について考えよう．この素イデアルは k の素イデアル P が存在して，この P からウルトラパワーによってできた $^*P$ である場合，(このとき $^*P$ が素イデアルであるということは，もとの構造とウルトラパワーで作られた構造とが同じ命題をみたすことから明らかである）この場合 $^*P$ のことを $^*k$ の standard 素イデアルとい

う．それからこのようにしては作られない $^*k$ の素イデアル，この場合この素イデアルを nonstandard な素イデアルという 2 通りの場合が考えられる．ここで注意すべきことは nonstandard な素イデアルといってもわれわれのウルトラパワーの構造のなかに入っている素イデアルである．

$^*k$ のアルキメディアン valuation のときは standard な valuation しかない．なぜならば k のアルキメディアン valuation は定理 5 により有限個しかなく，それを $v_1, \cdots, v_n$ とすれば

$$\forall v(v \text{ が } k \text{ のアルキメディアン valuation} \\ \rightarrow v \sim v_1 \vee v \sim v_2 \vee \cdots \vee v \sim v_n)$$

はもともとの構造 $\mathcal{T}$ では成立している．したがってウルトラパワーの構造 $\mathcal{S}$ でも

$$\forall v(v \text{ が } {}^*k \text{ のアルキメディアン valuation} \rightarrow v \sim {}^*v_1 \vee \cdots \vee v \sim {}^*v_n)$$

が成立し，$^*v_1, \cdots, {}^*v_n$ が $^*k$ のすべてのアルキメディアン valuation であることがわかる．すなわち $^*k$ のすべてのアルキメディアン valuation は standard である．

さて最初に $v = v_P$ が nonstandard な素イデアル P によってあたえられる場合を考えよう．いま $k^\times$ を以前と同じく k から 0 をのぞいてできるものを乗法の群として考えたものとしよう．いま $a \in k^\times$ なる a をとって考えよう．そのとき (a) を割る素イデアルの数は有限個である．これを $P_1, \cdots, P_n$ とする．k で

$$\forall P(P \text{ が } k \text{ の素イデアルで } P|(a) \rightarrow P = P_1 \vee \cdots \vee P = P_n)$$

が成立するから，$^*k$ で

$$\forall P(P \text{ が } {}^*k \text{ の素イデアルで } P|(a) \rightarrow P = {}^*P_1 \vee \cdots \vee P = {}^*P_n)$$

が成立して (a) を割る $^*k$ の素イデアルは standard であることがわかる．したがっていま P は nonstandard な素イデアルであるから

$$v_P(a) = 0$$

であることがわかる（この v_P は前節最後の記号法であることに注意），ゆえに v_P は k の上ではトリビアルすなわち恒等的に 0 である．

つぎに $v=v_P$ が standard な素イデアル P によってあたえられるときを考えよう．このときは v_P は k の上でトリビアルではない．われわれは k の上でトリビアルな別な valuation $\mathfrak{o}_P$ をつぎのごとく定義することにする．

$$\mathfrak{o}_P'=\{a\in{}^*k\,|\,a=0 \text{ または } v_P(a) \text{ が負の無限大でない}\}$$

ここに v_P は前節最後の記号法であることに注意されたい．また負の無限大というのは nonstandard な整数で負の無限大になるという意味である．$\mathfrak{o}_P'$ のなかに 0 を入れたのは $v_P(0)=\infty$ とおいて ∞ を正の無限大のなかにくり入れると考えてもよい．以下そのようにとり扱うこととする．$\mathfrak{o}_P'$ は明らかに $^*k$ における v-環になっている．いま $\mathfrak{o}_P$ を k の v-環とすると

$$\mathfrak{o}_P\subseteq\mathfrak{o}_P' \text{ かつ } k\subseteq\mathfrak{o}_P'$$

であることがわかる．（k の元の v_P の値は有限である）v_P' を $\mathfrak{o}_P'$ から作られた valuation であるとすると $k\subseteq\mathfrak{o}_P'$ であるからこの v_P' は k の上ではトリビアルである．この valuation の作る極大イデアル $\mathfrak{p}_P'$ は

$$\mathfrak{p}_P'=\{a\in{}^*k\,|\,v_P(a) \text{ が正の無限大（}\infty \text{ を含む）}\}$$

となっている．最後に valuation v_P' の値になっている群は Z を有理整数の全体とすると，v_P の $^*k$ についての値は $^*Z$ であり，v_P' の値はちょうど $^*Z/Z$ の元をとることになる．この $^*Z/Z$ を今後 Z_∞ と書くことにする．もっと正確にいえば，$\phi:{}^*Z\to Z_\infty$ を $^*Z\to{}^*Z/Z$ なる準同型とすれば

$$v_P'(a)=\phi v_P(a) \qquad a\in{}^*k^\times \text{ について}$$

が成立するものと思ってよい．

さてつぎに $|a|_P$ を $^*k$ の1つのアルキメディアン valuation とする．いま，$|\ \ |$ という記号を用いたのはいまのところアルキメディアン valuation とアルキメディアンでない valuation とをまったく異なったふうにとり扱っているので，記号法をまったくかえたほうが自然であるからである．$|\ \ |_P$ の P もあまり意味がなく，いろいろなアルキメディアン valuation のうちの 1 つを表わすために用いただけである．このとき

$$a\in{}^*k \text{ について } |a|_P\in{}^*R$$

となる．ここで R は前と同じく実数体を意味する．いま R_0 を

$$R_0=\{a\in{}^*R\,|\,a\text{ は有限}\}$$

とおいて,

$$R_\infty={}^*R/R_0$$

と定義し,　　ϕ は ${}^*R\rightarrow{}^*R/R_0$

なる準同型とする.

このとき ϕ は明らかに R_∞ に順序をあたえる. 以下においては R_∞ はこの意味で順序のついた群と考える. いますべての $a\in{}^*k^\times$ について

8.1
$$v_P'(a)=-\phi\log|a|_P$$

と定義する. ここに $|a|_P\in{}^*R$ であって, われわれのウルトラパワーの構造の正の実数について log はやはり定義されているから

$$\log|a|_P\in{}^*R$$

となる.

いまこの v_P' がアルキメディアンでない ${}^*k$ の valuation になり, その値の群が R_∞ となることを証明しよう.

いま任意の $a,b\in{}^*k^\times$ をとってくると

$$v_P'(ab)=-\phi\log|ab|_P=-\phi(\log|a|_P+\log|b|_P)$$
$$=-\phi\log|a|_P-\phi\log|b|_P=v_P'(a)+v_P'(b)$$

となる. ここに log についての性質は R で成立しているものは ${}^*R$ でも成立していることに注意すべきである. あとに残るのは

$$a+b\neq0$$

と仮定して　　$v_P'(a+b)\geq\min(v_P'(a),v_P'(b))$

を証明すればよい.

一般性を失うことなしに　　$v_P'(a)\leq v_P'(b)$

すなわち　　$\log|a|_P\geq\log|b|_P$

を仮定してよい. このとき

$$v_P'(a+b)=v_P'(a)+v_P'\left(1+\frac{b}{a}\right)$$
$$=-\phi\log|a|_P-\phi\log|1+b/a|_P$$

であるから, $-\phi\log|1+b/a|_P$ が R_∞ で負でないこと, すなわち $\log|1+b/a_P$

が正の無限大でないことを証明すればよい.

仮定により $\log|a|_P \geq \log|b|_P$

ゆえに $|b/a|_P \leq 1$

ゆえに $\log|1+b/a|_P \leq \log 2$

これによって証明は終った.

すべての R_∞ の元が v_P' の値になっていることを証明するためには, まず $*Q$ の元 a をとってくれば

$$|a|_P = a$$

(定理 5 において $*k$ の基礎体 $*Q$ は $*C$ のなかで $*k$ をどんなふうにうめ込もうとも自分自身にうつる.)

いま $*R$ の R_0 による勝手な剰余類をとってくる. もしこれが R_0 自身ならば $a \in N$ なる a をとればよいから明らかである. つぎにこの剰余類のなかに負の無限大 $-x$ が入っているときを考える. $(x \in *R)$

いま $x \leq \log|a+1|_P = \log(a+1)$ であるような最小な $a \in *N$ を考えると, $\log|a+1| - \log|a| = \log|1+1/a|$ は有限であり, x, $\log|a|_P$, $\log|a+1|_P$ はすべて同じ剰余類に属し, ゆえにこの剰余類に $v_P'(a)$ なる値が入っていることがわかる. つぎにもし考えている剰余類が正の無限大の元だけしかもっていないときは, $v_P'(a)$ の代りに $v_P'(b)$ と考えればよい. ここに $b=1/a$ で $a \in *N$ とすればよい.

v_P' の v-環 $\mathfrak{o}_P'$ は

$$\mathfrak{o}_P' = \{a \in *k \mid v_P'(a) \geq 0\} = \{a \in *k \mid \psi\log|a|_P \leq 0\}$$

によってあたえられる. ここに $\log 0 = -\infty$ とおく. したがって $a \in \mathfrak{o}_P'$ であるためには, $\log|a|_P$ は有限か負の無限大でなければならない. すなわち $|a|_P$ は有限でなければならない. 同様に $\mathfrak{o}_P'$ の極大イデアル $\mathfrak{p}_P'$ は

$$\mathfrak{p}_P' = \{a \in *k \mid |a|_P \text{ が無限小}\}$$

によってあたえられる. 無限小の全体はしばしば 0 のモナドといわれる.

$$k^\times \subseteq \mathfrak{o}_P' - \mathfrak{p}_P'$$

から v_P' が k の上でトリビアルであることがふたたび確認される.

9.　induced valuation

さていま K を k の上の超越次元 1 の拡大体，すなわち 1 変数の関数体であって $^*k$ の部分体になっているものとしよう．たとえば §6 で考えた Γ の generic point になっているような $^*k\times{}^*k$ の nonstandard な点 (ξ, η) をとってきて $k(\xi,\eta)$ を考えると，そういう K が得られる．ここでわれわれのウルトラパワー $\mathcal{S}$ のなかで考えるとこの K は $\mathcal{S}$ のなかに入っていない external なものになっている．たとえば $k(\xi,\eta)$ は external なものである．つぎに k が K のなかで代数的に閉じていることを注意しておく．これは k が $^*k$ のなかで代数的に閉じていることをいえばよいが，もし k の代数方程式が $^*k$ で根をもてば，k と $^*k$ とでは同じ理論が成立するから k ですでに根をもたなければならないことから明らかである．

さて v を k の上の（k の上ではトリビアルという意味）$^*k$ のアルキメディアンでない valuation としよう．ここでは v は internal かもしれないしまた external かもしれない．$\mathfrak{o}_v$，$\mathfrak{p}_v$ をこの v の v-環および極大イデアルとする．v を K の上に制限すれば，これは k ではトリビアルな K の valuation になる．これを V と書くことにしよう．V の v-環を $\mathfrak{O}_V$，極大イデアルを $\mathfrak{P}_V$ と書くことにすれば明らかに

$$\mathfrak{O}_V=\mathfrak{o}_v\cap K, \qquad \mathfrak{P}_V=\mathfrak{p}_v\cap K$$

が成立する．

V が K の上でトリビアルでない必要十分条件は，

$$K-\mathfrak{o}_v\neq\phi$$

なこと，すなわちある $a\in K^\times$ があって $v(a)>0$ なることである．

さて，ここで前節で導入された valuation について考えることにしよう．いま P を $^*k$ の nonstandard な素イデアルとして $v=v_P$ とする．このとき v_P が K のトリビアルでない valuation を作る条件は，ある $a\in K^\times$ について $v_P(a)>0$ なことである．いま a_0 を $K^\times$ の元で $v_P(a)$ が正でその内で一番小さいものとすれば

9.1 $$V_P(a)=\frac{v_P(a)}{v_P(a_0)}\qquad \text{任意の } a\in K^\times \text{ について}$$

とおけば V_P の値はつねに Z（有理整数環）の元となりこれが valuation になることは明らかであろう．

さてつぎに $v=v_P$ が standard な素イデアルから得られるときを考えよう．このときは v_P' が K でトリビアルでない必要十分条件は $v_P(a)$ が少なくとも $a\in K^\times$ なる a の 1 つで無限大になることである．このときは，$v_P'(a)$，$a\in K^\times$ が作る群は Z と同型な Z_∞ の部分群となる．$a_0\in K^\times$ を $v_P'(a_0)$ が正のなかで最小のものをとって

9.2 $$V_P(a)=\frac{v_P'(a)}{v_P'(a_0)}\qquad a\in K^\times \text{ なる } a \text{ について}$$

とおけば，V_P は valuation で値は Z からとる．この右辺は正確にいえば $n\in Z$ なる n で

$$v_P'(a)=n\cdot v_P'(a_0)$$

をみたすものである． $Z_\infty={}^*Z/Z$

であるから $v_P(a)=n\cdot v_P(a_0)+r$

でここで $r\in{}^*Z$ と書くことができる．ゆえに

9.3 $$V_P(a)={}^0\!\left(\frac{v_P(a)}{v_P(a_0)}\right)\qquad a\in K^\times \text{ について}$$

と書いても同じことになる．

最後に $v=v_P$ で v_P がアルキメディアンである場合を考えよう．ここで K に制限された valuation がトリビアルでない必要十分条件はある $a\in K^\times$ なる a について $\log|a|_P$ が無限になることであり，これはさらにある $a\in K^\times$ について $|a|_P$ が無限になることである．この仮定のうえで，$v_P'(a)$，$a\in K^\times$ が作る R_∞ の部分群はふたたび Z と同型になる．われわれは $a_0\in K^\times$ を $v_P'(a_0)$ が正のなかで最小になるように選んで，$V_P(a)$ を 9.2 によって定義する．ここでふたたび，右辺は $n\in N$ で $v_P'(a)=nv_P'(a_0)$ となる n のことであると定義するのである．8.1 によりこれはつぎの式と同等になる．

$$\phi(\log|a|_P-n\log|a_0|_P)=0$$

すなわち $\log|a|_P-n\log|a_0|_P=r$ で r は有限となる．すなわち $r/\log|a_0|_P$

は無限であり，

9.4 $$V_P(a)=\left(\frac{\log|a|_P}{\log|a_0|_P}\right) \qquad a\in K^\times \text{ について}$$

となる．しかしながら 9.2 は 9.3 や 9.4 より一層正確であるので，われわれは将来のためにつぎのごとくしておこう．

9.5 $$V_P(a)=\frac{v_P(a)}{v_P(a_0)}-\frac{r}{v_P(a_0)}$$

ここで，P は standard 素イデアルで $r\in N$.

9.6 $$V_P(a)=\frac{\log|a|_P}{\log|a_0|_P}-\frac{r}{\log|a_0|_P}$$

ここで P はアルキメディアン valuation を表わして r は有限．

$^*k$ の相異なる 2 つの valuation が K のトリビアルでない同じ valuation をひき起こすことがありうるということを注意しておく．

10.　有理関数体の場合

さて K が k の上の 1 変数の有理関数体（またはそれと同型）である場合を考えよう．このような K は k に $^*k-k$ のいかなる元をつけ加えても得られる．われわれは以下に k の上でトリビアルな K の valuation（これを今後 K/k の valuation という）はすべて $^*k$ の internal valuation からひき起こされることを証明しよう．

$$K=k(\omega) \quad \text{で} \quad \omega\in{}^*k-k$$

であるとしよう．x を未知数として χ を $k(x)$ から $k(\omega)$ への x を ω へうつし，k の元は自分自身にうつす同型対応であるとする．$p(x)\in k[x]$ を $k[x]$ で既約な多項式であるとする．$p(x)$ はつぎのように $k(x)$ の valuation w_p を定義する．$q(x)\in k[x]$ を恒等的に 0 でないものとして

$$q(x)=(p(x))^m s(x)$$

で $s(x)$ は $p(x)$ と素なものとする．そのとき

$$w_p(q(x))=m$$

と定義し，w_p を普通のように $k(x)$ に拡張するのである．この w_p によっ

て $k(\omega)$ の valuation が

$$W_p=w_p\chi^{-1} \text{ または } W_p(q(\omega))=W_p(q(x))=m$$

によって定義される．とくに　$W_p(p(\omega))=1$

となる．

さて $\alpha=p(\omega)$ とおいて

$$(\alpha)=\prod P_j^{\nu_j}$$

をイデアル (α) の $^*k$ における素イデアルへの分解であるとする．ここに $\prod P_j^{\nu_j}$ はわれわれのウルトラパワー $\mathcal{S}$ のなかでキチンと表現することができる．したがってここに現われる P_j の数は有限である場合も無限である場合もあるが，いずれにしても $^*N$ の元としてキチンと表わされるわけである．さてこの (α) の分解のなかに nonstandard な素イデアル $P=P_j$ が $\nu>0$ で表わされるときを考えよう．

われわれは V_P と W_p とが一致することを証明しよう．

さて

10.1　　$$p(x)=a_0+a_1x+\cdots+a_nx^n,\quad a_n\neq 0, n\geq 1$$

であるとしよう．まず $\beta\in k[\omega]$ なるすべての β について $v_P(\beta)\geq 0$ であることを証明しよう．最初に $\beta=\omega$ の場合を考え $v_P(\omega)<0$ であるとしよう．しかし，$v_P(a_j)=0$ が $j=0,1,\cdots,n$ で $a_j\neq 0$ でない j に対して成立するから，

$$v_P(p(\omega))=\min_j v_P(a_j\omega^j)<0$$

となって仮定に反する．ゆえに $v_P(\beta)\geq 0$ は $\beta=\omega$ に対して成立しており，したがって $q(\omega)=b_0+b_1\omega+\cdots+b_l\omega^l\in k[\omega]$ なるいかなる $q(\omega)$ に対しても成立している．

つぎに上のように $q(x)=(p(x))^m\cdot s(x)$ と分解したとき

$$v_P(s(\omega))=0$$

であることを証明しよう．なぜならば

$$p(x)q(x)+s(x)h(x)=1$$

のように $q(x),h(x)\in k[x]$ がとれるから

$$0=v_P(1)=v_P(p(\omega)q(\omega)+s(\omega)h(\omega))$$
$$\geq \min(v_P(p(\omega)q(\omega)), v_P(s(\omega)h(\omega)))$$

しかし　$$v_P(p(\omega)q(\omega))=v_P(p(\omega))+v_P(q(\omega))\geq 1$$

だから　$$0=v_P(s(\omega)h(\omega))=v_P(s(\omega))+v_P(h(\omega))$$

となり　$$v_P(s(\omega))=v_P(h(\omega))=0$$

がでてくる．ゆえに

$$v_P(q(\omega))=m\,v_P(p(\omega))=m\,v_P(\alpha)$$

となり $v_P(y)$ は $y=\alpha$ で正のなかで最小の値をとることがわかる．したがって 9.1 の a_0 として $\alpha=p(\omega)$ をとることができ，$\beta=q(\omega)$ については

$$V_P(\beta)=\frac{v_P(\beta)}{v_P(\alpha)}=m=W_p(\beta)$$

が成立し $k[\omega]$，したがって $k(\omega)$ の上で

$$V_P=W_p$$

がいえる．

さてこんどは，standard な素イデアル $P=P_j$ が (α) の素因数分解のなかに $\nu=\nu_j$ という正の無限大の次数で現われている場合を考えよう．ここにやはり $p(x)$ は 10.1 で表わされ $\alpha=p(\omega)$ である．この場合は $v_P(\omega)$ は負の無限大ではありえない．なんとならば $v_P(a_j)$ は $a_j\neq 0$ ならば有限でそれゆえ $v_P(a)=\min\,(v_P(a_j\omega^j))$ が負の無限大になってしまうからである．したがって $v_P(q(\omega))$ は $q(x)\in k[x]$ なる q について，有限か正の無限大のいずれかになる．またさらに

$$0=v_P(1)=v_P(p(\omega)q(\omega)+s(\omega)h(\omega))$$
$$\geq \min(\nu+v_P(q(\omega)), v_P(s(\omega))+v_P(h(\omega)))$$

となる．ここで $\nu=v_P(\alpha)$ とする．この式から $v_P(s(\omega))$ は正の無限大ではありえない．したがって有限であることがわかる．もし

$$\beta=q(\omega)=(p(\omega))^m s(\omega)$$

とすれば　$$v_P(\beta)=m\nu+r \quad \text{で} \quad r\in Z$$

となる．したがって $\phi{:}{}^*Z\to Z_\infty$ を用いれば

$$v_P'(\beta)=mv_P'(\alpha)$$

となり，$v_P'(\alpha)$ は v_P' の正の値のなかで最小なことがわかり，9.2 の a_0 として α がとれることがわかる．ゆえに

10.2
$$V_P(\beta)=\frac{v_P'(\beta)}{v_P'(\alpha)}=m=W_p(\beta)$$

がいえ，
$$V_P=W_p$$
が $k[\omega]$ で，したがって $k(\omega)$ で成立することがわかる．

最後に $\alpha=p(\omega)$（この $p(x)$ は 10.1 であたえられたものである）が $^*k$ のアルキメディアン valuation P で無限小である場合を考えよう．この場合は $|\omega|_P$ がもし無限だとすると

$$|a_n|_P=\left|\frac{p(\omega)}{\omega^n}-\frac{a_0}{\omega^n}-\cdots-\frac{a_{n-1}}{\omega}\right|_P$$

は無限小になってしまって矛盾するので $|\omega|_P$ は有限でなければならない．ゆえに $q(x)\in k[x]$ なる q について，$|q(\omega)|_P$ が有限であることがこれからただちにでる．また

$$p(x)q(x)+s(x)h(x)=1$$

を考えて $|p(\omega)q(\omega)|_P$ が無限小のことから

$$|s(\omega)h(\omega)|_P\simeq 1$$

のことがでる．ここに $a\simeq b$ とは $a-b$ が無限小のことを意味する．これから $|s(\omega)|_P$ と $|h(\omega)|_P$ は有限であるが無限小でないことがわかる．したがって $\beta=q(\omega)\neq 0$ には

$$\log|\beta|_P=\log|(p(\omega))^m s(\omega)|_P=m\log|\alpha|_P+r$$

ここに $r=|s(\omega)|_P$ は有限である．$\phi:{}^*R\to R_\infty$ を考えれば（8.1 参照）

$$v_P'(\beta)=mv_P'(\alpha)$$

したがって $v_P'(\alpha)$ は正の値のなかで最小なることがわかる．したがって 9.2 の a_0 として α をとってきてよく，10.2 がこの場合にも得られた．

さてわれわれは素の $p(x)\in k[x]$ があたえられたとき上に考えた 3 つの場合の少なくとも 1 つが実際に成立することを証明することにする．すなわち (α) が nonstandard な素の因子を正の次数でもっているか，standard な素の因子を正の無限大の次数でもっているか，それともあるアルキメディ

アン P があって，$|\alpha|_P$ が無限小となるかのいずれかが 1 つは成立する．

いま μ は k の素イデアルを重複なしに並べたものとする．このとき $^*\mu$ は $^*k$ の（internal）素イデアルを重複なしに並べたものとなる．

$$^*\mu=\{P_0, P_1, \cdots, P_n, \cdots\}$$

n が有限ならば P_n は standard になり，n が無限ならば P_n は nonstandard になる．

さて $(\alpha)=(p(\omega))$ がどんな nonstandard 素イデアルも正の次数では含んでいないとする．このときは S_α を (α) に正の次数で現われる素イデアルの集合とすると，S_α の元の個数は $^*N$ の元となる．いま S_α の個数がじつは有限であることをいおう．もし S_α が空ならばそれでよい．S_α が空でないとすれば，$j\geq n$ ならば $P_j \notin S_\alpha$ であるような最初の $n\in{}^*N$ が存在する．($^*N$ の最小値の原理)．明らかに

$$n\geq 1 \text{ で } P_{n-1}\in S_\alpha$$

である．ゆえに n は有限であって S_α が有限であることがわかる．したがって，もし (α) が nonstandard な素イデアルを正の次数でももっていず，standard な素イデアルを正の無限大の次数でももっていないとすれば，(α) の分子の因数分解は standard な素イデアルの有限個の積でできており，したがって standard であることがわかる．

$$(\alpha)=J_1/J_2$$

と書いて J_1 は standard，J_2 は $^*k$ のイデアルである．

さて k の類数は有限であるから，standard なイデアル J_3 があって J_1J_3 は主イデアルとなり，　　$J_1J_3=(\gamma)$，　$\gamma\in k$

となる．いま $^*k$ について考えてもこの関係は成立しており J_2J_3 も主イデアルになり　　$J_2J_3=(\delta)$

とおけば δ は $^*k$ の整数であり，$\alpha=\gamma/\varepsilon\delta$

で ε は $^*k$ の unit となる．または

$$\alpha=\gamma/\zeta, \quad \zeta=\gamma/\alpha$$

となる．

さてこの場合に $|\alpha|_P$ は少なくとも 1 つの k のアルキメディアン valuation P について無限小となることを証明しよう．

もしそうでないとすれば，$|\zeta|_P=|\gamma/\alpha|_P$ はすべての $^*k$ のアルキメディアン valuation で有限となる．すなわち $\zeta=\zeta^{(1)},\cdots,\zeta^{(l)}$ を ζ の有理数体の上の共役なる数の全部とすると $|\zeta^{(1)}|,\cdots,|\zeta^{(l)}|$ は全部有限となる．ここに絶対値 $|\ \ |$ は特別な $^*k$ の $^*C$ へのうめこみ方に対してとられたものである．このことは $\zeta^{(1)},\cdots,\zeta^{(l)}$ の基本対称式で表わされるものを $s_1,\cdots,s_l$ と書けば $s_1,\cdots,s_l$ はすべて有限の整数，したがって standard な整数である．ζ は多項式 $z^l-s_1z^{l-1}+\cdots+(-1)^ls_l$ の根であるから，ζ 自身 standard でなければならず，$\zeta\in k$ となる．これから $\alpha=p(\omega)$ が standard となり，これは $p(x)$ の次数が正であることと矛盾する．したがってわれわれは，以前に考えた 3 つの場合の少なくとも 1 つが成立して W_p が $^*k$ の internal valuation の 1 つからひき起こされることがわかった．

しかしながら，$k(\omega)/k=K/k$ の valuation で $k[x]$ の素の多項式 $p(x)$ でひき起こされない唯 1 つの例外がある．この例外は無限大における valuation である．しかしこの valuation は $\omega'=1/\omega$ とおいて，K を $k(\omega')$ と考えたうえで $p(x')=x'$ なる多項式であたえられる．したがってわれわれは K/k なるすべての valuation が $^*k$ の internal valuation でひき起こされることがわかった．

11. divisor の大きさ

さてこんどは k の上の超越次数が 1 であるような $^*k$ の任意の部分体 K について考えることにしよう．(以下に代数学の知識を仮定する．)

R_+ は正の実数の乗法群とし，$^*R_+$ はそのウルトラパワーによる拡大であるとする．$^*R_+$ のなかで R_l を有限ではあるが無限小ではない部分とする．われわれは R_l を log で有限な部分と呼ぶことにしよう．これはこの部分が log をほどこしたとき有限な部分になっているからである．R_l は $^*R_+$ の乗法についての部分群になっている．$R_{+\infty}$ を商群 $^*R_+/R_l$ によって定義し，

$$\theta: {}^*R_+ \to R_{+\infty}$$

をその準同型とする．

λ を $y=\log x$ によって定められる $^*R_+$ から $^*R$ の上への写像とする．これは乗法群 $^*R_+$ から加法群 $^*R$ の上への同型写像である．この写像は $R_{+\infty}$ から R_∞ の上への同型写像 λ_0 をひき起こす．そしてこの同型が $R_{+\infty}$ の上の順序を定める．

いま D を K を関数体としての divisor の集合とする．$K^\times$ の元 α に対して，α の divisor を α の関数と考えて $[\alpha]$ によって表わすことにする．われわれは D から $R_{+\infty}$ のなかへの写像 σ を定義しよう．

A が D のなかの整の divisor であって，

$$A=\prod A_j^{\omega_j}$$

で，A_j は素の divisor で ω_j は正であるとする．近似定理を用いれば，$K^\times$ の 2 元 α,β を作って，$[\alpha]$ と $[\beta]$ の分子の最大公約 divisor がちょうど A であるしそのうえ $[\alpha]$ と $[\beta]$ のなかの A_j の次数がちょうど ω_j であるようにできる．いま (α) と (β) とが α および β によって $^*k$ のなかで生成される（整または分数）イデアルとせよ．このとき (α) と (β) の分子の最大公約 divisor は $^*k$ のなかの整の internal イデアルになる．これを $J_{\alpha,\beta}$ と書くことにする．

$$J_{\alpha,\beta}=\prod P_j^{\nu_j}$$

を $J_{\alpha,\beta}$ の素因数分解とする．各々の P_j に対して，NP_j を $^*Q$ に相対的な P_j のノルムを表わすものとして，

$$|J_{\alpha,\beta}|=\prod (NP_j)^{-\nu_j}$$

とおこう．$|J_{\alpha,\beta}|$ に $|\alpha|_P$, $|\beta|_P$ がともに無限小であるような $^*k$ のすべてのアルキメディアン valuation P について $\max(|\alpha|_P, |\beta|_P)$ をかけてできたものを $s(\alpha,\beta)$ と名づけよう．すなわち

11.1　$$s(\alpha,\beta)=|J_{\alpha,\beta}|\prod \max(|\alpha|_P, |\beta|_P)$$

ここに右辺の積は上にのべたような P について行なうものとする．

われわれは $\sigma(A)$ を

11.2 $$\sigma(A)=\theta(s(\alpha,\beta))=\theta(|J_{\alpha,\beta}|)\prod\theta(\max(|\alpha|_P,|\beta|_P))$$

によって定義する．ここに $\theta: {}^*R_+ \to R_{+\infty}$ は前にのべた同型写像である．

$\sigma(A)$ のことを A の**大きさ**という．

われわれは $\sigma(A)$ が α,β のとり方によらないことを証明しなければならない．すなわち $K^\times$ の別の 2 元 α',β' で A に関しては α,β と同じ条件をみたしているものをとってきたとき

$$\theta(s(\alpha',\beta'))=\theta(s(\alpha,\beta))$$

または同じことであるが

$$s(\alpha,\beta)/s(\alpha',\beta') \text{ が log の意味で有限}$$

であることを証明しなければならない．

(α,β) と (α',β') が対称的であることを心にとめて，問題をつぎのごとくに 2 つに分けることにする．

（i） P を $|\alpha|_P,|\beta|_P$ がともに無限小になるようなアルキメディアン valuation とする．このとき，$|\alpha'|_P,|\beta'|_P$ はともに無限小であって

$$\max(|\alpha'|_P,|\beta'|_P)/\max(|\alpha|_P,|\beta|_P)$$

は log の意味で有限である．

（ii） イデアル $J_{\alpha',\beta'}/J_{\alpha,\beta}$ は standard である．

実際にもし（i）がみたされていてさらに（i）で (α,β) と (α',β') をとりかえたものもみたされていれば，11.2 の右辺の積 $\prod\theta(\max(|\alpha|_P,|\beta|_P))$ はそれに対応する (α',β') に対する積と等しくなる．さらにもし $J_{\alpha',\beta'}/J_{\alpha,\beta}$ が standard ならば $|J_{\alpha',\beta'}|/|J_{\alpha,\beta}|$ は log の意味で有限になり，

したがって $$\theta(|J_{\alpha',\beta'}|)=\theta(|J_{\alpha,\beta}|)$$

となる．これから $$\theta(s(\alpha,\beta))=\theta(s(\alpha',\beta'))$$

がでてくる．

さて，つぎのごとく定義しよう．

11.3 $$[\alpha]=\prod Q_j^{\kappa_j},\quad [\beta]=\prod R_j^{\lambda_j}$$
$$[\alpha']=\prod S_j^{\mu_j},\quad [\beta']=\prod T_j^{\rho_j}$$

ここでわれわれはその次数が 0 でない divisor だけをここにとり入れてあ

るものとする.

さて $|\alpha|_P, |\beta|_P$ がともに無限小になるようなアルキメディアン valuation としよう. そのとき P は K/k に α, β がともに正になるような valuation Q をひき起こす. そのとき Q を divisor とみなして, それは A_j の 1 つと, また Q_j の 1 つと, またさらに R_j の 1 つと一致する. われわれは一般性を失うことなしにこのすべての場合に $j=0$ であると仮定する. そのとき $\omega_0=\kappa_0=\lambda_0>0$ となる. 同じことを α', β' に考えて Q が S_0, T_0 と一致し $\omega_0=\mu_0=\rho_0$ であると思ってよい. α_0 を §9 のように選べば (9.6 を参照) つぎの式を得る.

11.4
$$\begin{aligned}\omega_0\log|\alpha_0|_P &= \log|\alpha|_P - r_1\\ &= \log|\beta|_P - r_2\\ &= \log|\alpha'|_P - r_3\\ &= \log|\beta'|_P - r_4\end{aligned}$$

ここに $\log|\alpha_0|_P, \log|\alpha|_P, \log|\beta|_P, \log|\alpha'|_P, \log|\beta'|_P$ は負の無限大であり, r_1, r_2, r_3, r_4 は有限である. ゆえにつぎの式が成立する.

11.5
$$\begin{aligned}|\alpha|_P &= e^{r_1}(|\alpha_0|_P)^{\omega_0}\\ |\beta|_P &= e^{r_2}(|\alpha_0|_P)^{\omega_0}\\ |\alpha'|_P &= e^{r_3}(|\alpha_0|_P)^{\omega_0}\\ |\beta'|_P &= e^{r_4}(|\alpha_0|_P)^{\omega_0}\end{aligned}$$

さて $|\alpha_0|_P$ は無限小であるから, つぎの式が得られる.

$$\max(|\alpha|_P, |\beta|_P)=c_1(|\alpha_0|_P)^{\omega_0}, \qquad \max(|\alpha'|_P, |\beta'|_P)=c_2(|\alpha_0|_P)^{\omega_0}$$

ここで, c_1, c_2 は log の意味で有限である. これで (i) が証明された.

さて, (ii) を証明するために $^*k$ のイデアル $(\alpha), (\beta), (\alpha'), (\beta')$ を考えることにする. さて nonstandard な素イデアル P が (α) と (β) に正の次数 ν_1, ν_2 で現われるとする. このとき P は K に valuation Q をひき起こし, この Q は Q_j の1つと一致し (11.3 参照) またさらに R_j の 1 つと一致する. $Q=Q_0=R_0$ とする. しかしそうすれば Q はまた A_j の 1 つとも一致する. $Q=A_0$ としよう. α_0 を §9 の nonstandard 素イデアルの場合

のように選んで 9.1 からわれわれはつぎの式を得る.

11.6 $$\omega_0=\kappa_0=\lambda_0=\frac{\nu_1}{v_P(\alpha_0)}=\frac{\nu_2}{v_P(\alpha_0)}$$

ここで $v_P(\alpha_0)$ は standard または nonstandard な自然数である. ゆえに $\nu_1=\nu_2$ となる. 同様にして Q は $[\alpha'],[\beta']$ の分子の素 divisor のなかに現われ, たとえば $Q=S_0=T_0$ とすれば, $\mu_0=\rho_0=\omega_0$ となる. さらに, $(\alpha'),(\beta')$ の素因数分解のなかの P の次数を $\nu_3=\nu_4$ とすれば

$$\omega_0 v_P(\alpha_0)=\nu_3=\nu_4$$

となり,
$$\nu_1=\nu_2=\nu_3=\nu_4$$
が得られた.

われわれはすべての nonstandard 素イデアルについてそれが $J_{\alpha,\beta}$ を割ればちょうど同じ次数で $J_{\alpha',\beta'}$ を割ることを証明した. いま H を $J_{\alpha,\beta}$ を $J_{\alpha',\beta'}$ より高い次数で割る素イデアルの集合であるとする. この H は internal である. しかも H の元は standard な素イデアルだけである. H は空かもしれない. もしそうでないとしても H は高々有限であることを証明しよう.

このために
$$^*\mu=\{P_0,P_1,P_2,\cdots\}$$
を §10 で定義した $^*k$ の internal 素イデアルの列としよう. n をすべての $j\geq n$ について $P_j\notin H$ となるような最小の n としよう. もし n が無限ならば $P_{n-1}\in H$ となるがこれは P_{n-1} が nonstandard になるから不可能である. したがって n は有限であり H も有限であることがわかる.

さていま $P\in H$ とする. P が $(\alpha),(\beta)$ の分子を ν_1,ν_2 の次数で割るものとする. ここで $\nu_1>0$, $\nu_2>0$ である. もし ν_1, ν_2 が有限であれば, P は $J_{\alpha,\beta}/J_{\alpha',\beta'}$ の分子のなかに高々有限の次数でしか現われない. このとき P は K の valuation Q をひき起こし, この Q は divisor として $[\alpha]$ と $[\beta]$ 双方の分子のなかに現われる. したがってわれわれは

$$Q=A_0=Q_0=R_0$$

(11.3 参照) と仮定してよく
$$\omega_0=\kappa_0=\lambda_0$$
となる. 同様にして
$$Q=S_0=T_0$$

としてよく

$$\omega_0=\mu_0=\rho_0$$

が得られる．α_0 を §9 のように選んで 9.5 を適用すれば

$$\omega_0 v_P(\alpha_0)=\nu_1-r_1=\nu_2-r_2=\nu_3-r_3=\nu_4-r_4$$

ここに r_1, r_2, r_3, r_4 は有限であり，P は $(\alpha'), (\beta')$ をちょうど ν_3, ν_4 の次数で割るのである．このことから

$$\min(\nu_1, \nu_2)-\min(\nu_3, \nu_4)=r$$

とすれば r は有限，すなわち $J_{\alpha,\beta}$ と $J_{\alpha',\beta'}$ とにおける P の次数の差は有限であることがわかる．したがって $J_{\alpha,\beta}/J_{\alpha',\beta'}$ の分子は standard なイデアルであることがいえ，対称性によりその分母も standard であることがわかって（ii）が証明された．

さてとくに $\alpha=\beta$ である場合を考えよう．このときは A はちょうど $[\alpha]$ の分子である．11.2 により

11.7　$$\sigma(A)=\theta(s(\alpha,\alpha))=\theta(\prod\min(|\alpha|_P, 1))$$

ここで P はこんどはアルキメディアン，アルキメディアンでないを問わず全部の internal valuation を走るのである．P がアルキメディアンでないとき $|\alpha|_P$ は (α) の素イデアルによる因数分解における P の次数が ν ならば $(NP)^{-\nu}$ で定義するのである．他方 α の**高さ**（height）は $^*k$ の数として

11.8　$$H(\alpha)=\prod\max(|\alpha|_P, 1)$$

によって定義される．

すべての $|\alpha|_P$ の積は 1 であるから

$$s(\alpha,\alpha)=(H(\alpha))^{-1}$$

が得られ，したがってつぎの式が得られる．

11.9　$$\sigma(A)=\theta((H(\alpha))^{-1})=(\theta(H(\alpha)))^{-1}$$

われわれはつぎに σ が整の divisor の半群の上で（じつは σ はまだこの上で定義されていないが）乗法群であることを証明しよう．A, B を 2 つの整の divisor であるとしよう．われわれはまず α, β を前のように選び，それから近似定理を用いて α', β' を同様の条件を B に対して選び，さらに 11.3 の記号においていかなる素の divisor Q_j も R_j ももしそれが A と B

とを同時に割るのでなければ S_j または T_j として現われないようにとる．このようにすると，その結果として，AB のなかのすべての素の divisor は AB に現われるのと同じ次数だけ $[\alpha\alpha']$ の分子に，また $[\beta\beta']$ の分子のなかに現われることになる．したがって 11.2 のほかにわれわれはつぎのものを得る．

11.10　　$\sigma(B)=\theta(s(\alpha',\beta'))=\theta(|J_{\alpha',\beta'}|)\prod\theta(\max(|\alpha'|_P,|\beta'|_P))$

11.11　　$\sigma(AB)=\theta(s(\alpha\alpha',\beta\beta'))=\theta(|J_{\alpha\alpha',\beta\beta'}|)\prod\theta(\max(|\alpha\alpha'|_P,|\beta\beta'|_P))$

ここでまた双方とも右辺の積はふさわしいアルキメディアン valuation の上だけにとられるのである．

$\sigma(AB)=\sigma(A)\sigma(B)$ を証明するためにはつぎの命題を証明すれば十分である．

（iii）　P を任意のアルキメディアン valuation とせよ．そのとき

$$\max(|\alpha\alpha'|_P,|\beta\beta'|_P) \text{ が無限小}$$

になる必要十分条件は $\max(|\alpha|_P,|\beta|_P)$, $\max(|\alpha'|_P,|\beta'|_P)$ の少なくとも 1 つが無限小になることである．しかももしこれが成立するときには

$$\max(|\alpha|_P,|\beta|_P)\cdot\max(|\alpha'|_P,|\beta'|_P)/\max(|\alpha\alpha'|_P,|\beta\beta'|_P)$$

は log の意味で有限となる．

（iv）　イデアル $J_{\alpha,\beta}J_{\alpha',\beta'}/J_{\alpha\alpha',\beta\beta'}$ は standard である．

証明はこの節の（ i ），（ii）の証明と平行して行なわれる．まず最初に

$$\max(|\alpha|_P,|\beta|_P) \text{ か } \max(|\alpha'|_P,|\beta'|_P) \text{ が無限小}$$

ならば，P はそれぞれ A か B を割る K/k の valuation（素の divisor）Q をひき起こすことが（ i ）の証明と同じようにわかる．これを用いて

$$Q \text{ が } AB \text{ を割る．}$$

したがって　　$\max(|\alpha\alpha'|_P,|\beta\beta'|_P)$ は無限小

になる．逆にもし $\max(|\alpha\alpha'|_P,|\beta\beta'|_P)$ が無限小ならば，すなわち

$$|\alpha\alpha'|_P \text{ も } |\beta\beta'|_P \text{ も無限小}$$

ならば，P は AB を割る Q，したがって A か B かの一方を割ることになる．このことから

$\max(|\alpha|_P, |\beta|_P)$ か，$\max(|\alpha'|_P, |\beta'|_P)$ かの少なくとも一方が無限小であることがわかる．ゆえに，$\omega_0 \geqq 0$ と $\zeta_0 \geqq 0$ とを Q が A と B とを割る次数であるとすれば（したがって ω_0 と ζ_0 との少なくとも一方は正である）．このとき

$$Q \text{ は } AB \text{ を } \omega_0+\zeta_0 \text{ の次数で割る．}$$

それゆえに 9.6 により適当な α_0 をとって，

11.12
$$\begin{aligned}\omega_0 \log|\alpha_0|_P &= \log|\alpha|_P - r_1 \\ &= \log|\beta|_P - r_2\end{aligned}$$

がもし $\omega_0>0$ ならば r_1, r_2 が有限で成立する．

しかしこれは $\omega_0=0$ であっても正しい．なぜならばこの場合 Q は $[\alpha]$ または $[\beta]$ の分母に現われることはできずしたがって，$\log|\alpha|_P$, $\log|\beta|_P$ は有限になるからである．同様にして

11.13
$$\begin{aligned}\zeta_0 \log|\alpha_0|_P &= \log|\alpha'|_P - r_3 \\ &= \log|\beta'|_P - r_4\end{aligned}$$

ここに r_3, r_4 は有限である．そして AB を考えることによって

11.14
$$\begin{aligned}(\omega_0+\zeta_0)\log|\alpha_0|_P &= \log|\alpha\alpha'|_P - r_5 \\ &= \log|\beta\beta'|_P - r_6\end{aligned}$$

ここに r_5, r_6 は有限である．これから

$$\max(|\alpha|_P, |\beta|_P) = c_1(|\alpha_0|_P)^{\omega_0}$$

$$\max(|\alpha'|_P, |\beta'|_P) = c_2(|\alpha_0|_P)^{\zeta_0}$$

$$\begin{aligned}\max(|\alpha\alpha'|_P, |\beta\beta'|_P) &= c_3(|\alpha_0|_P)^{\omega_0+\zeta_0} \\ &= c_3(|\alpha_0|_P)^{\omega_0}(|\alpha_0|_P)^{\zeta_0} \\ &= c_4 \max(|\alpha|_P, |\beta|_P)\max(|\alpha'|_P, |\beta'|_P)\end{aligned}$$

ここに c_1, c_2, c_3, c_4 は log の意味で有限でありこれで（iii）は証明された．

（iv）を証明するために，われわれはこんどもまず nonstandard な素イデアル P を考えることにしよう．もし

$$P \text{ が } J_{\alpha,\beta} \text{ を割る}$$

ならば，それは (α) と (β) の分子を割ることになる．したがって P は K/k

の $[\alpha]$ と $[\beta]$ とを割る valuation Q をひき起こす．このことから Q が $[\alpha']$, $[\beta']$ の分母を割れないことがわかり，したがって $[\alpha\alpha']$, $[\beta\beta']$ の分子を割ることがわかる．このことからさらに P が $(\alpha\alpha'), (\beta\beta')$ を割り，したがって

$$P \text{ は } J_{\alpha\alpha',\beta\beta'} \text{ を割る}$$

ことがわかる．同じ理由でもし P が $J_{\alpha',\beta'}$ を割ればそれはやはり $J_{\alpha\alpha',\beta\beta'}$ を割る．

さて

$$P \text{ が } J_{\alpha\alpha',\beta\beta'} \text{ を割る}$$

とせよ．このとき P は $[\alpha\alpha'], [\beta\beta']$ の分子を割る K/k の valuation Q をひき起こす．これから Q が AB を割ることがわかり，したがって A か B の少なくとも一方を割ることがわかる．一般性を失うことなしに

$$Q \text{ が } A \text{ を割る}$$

とする．これから Q が $[\alpha]$ と $[\beta]$ の分子を割ることがわかり，したがって P が (α) と (β) の分子を割り，Q が $J_{\alpha,\beta}$ を割ることがわかる．こうして，いずれの場合にも，

$$P \text{ が } J_{\alpha\alpha',\beta\beta'} \text{ を割ることは } P \text{ が } J_{\alpha\beta}J_{\alpha'\beta'} \text{ を割ることと同等}$$

であり，そして後者の場合には Q が AB を割る．

この仮定のもとで，$\omega_0 \geq 0$, $\zeta_0 \geq 0$ は Q が A および B を割る次数とせよ．このとき Q は AB を次数 $\omega_0+\zeta_0>0$ で割る．したがって 9.1 により適当な α_0 をとれば

11.15
$$\omega_0 v_P(\alpha_0)=\nu_1, \quad \zeta_0 v_P(\alpha_0)=\nu_2,$$
$$(\omega_0+\zeta_0)v_P(\alpha_0)=\nu_1+\nu_2$$

ここに ν_1, ν_2 は一方では P が (α), (β) の分子を割る次数であり，他方では $(\alpha'), (\beta')$ の分子を割る次数である．このことから

$$P \text{ が } J_{\alpha,\beta} \text{ を } \nu_2 \text{ の次数で,}$$
$$J_{\alpha',\beta'} \text{ を } \nu_1 \text{ の次数で,}$$
$$J_{\alpha\alpha',\beta\beta'} \text{ を } (\nu_1+\nu_2) \text{ の次数で割る}$$

ことがわかる．このことはイデアル

$$J_0=J_{\alpha,\beta}J_{\alpha',\beta'}/J_{\alpha\alpha',\beta\beta'}$$

が分子にも分母にも standard な素イデアルしかもっていないことを示している．前と同じように $^*\mu$ を用いることによって，これらのイデアルの数が有限であることを証明することができる．

P をこのイデアルの 1 つとしよう．もし P が $J_{\alpha,\beta}$ と $J_{\alpha',\beta'}$ を高々有限の次数で割るとすれば，P は J_0 の分子のなかに高々有限の次数でしか現われない．もしこのことが成立しないとすると P は K/k の素の divisor である valuation Q をひき起こす．このとき Q は A または B（または双方とも）を割り，いずれにしても AB を割る．Q が A を割るものとせよ．このときわれわれは $Q=A_0=Q_0=R_0$ と思ってよくしたがって $\omega_0=\kappa_0=\lambda_0$ は正であって，9.5 により適当な α_0 について

$$\omega_0 v_P(\alpha_0)=v_P(\alpha)-r_1=v_P(\beta)-r_2$$

で，r_1, r_2 は有限となる．同時に

$$\zeta_0 v_P(\alpha_0)=v_P(\alpha')-r_3=v_P(\beta')-r_4$$

$$(\zeta_0+\omega_0)v_P(\alpha_0)=v_P(\alpha\alpha')-r_5=v_P(\beta\beta')-r_6$$

ここで Q は B を $\zeta_0\geq 0$ の次数で割るものとする．このことから P が $J_{\alpha,\beta}$, $J_{\alpha',\beta'}$, $J_{\alpha\alpha',\beta\beta'}$ をそれぞれ有限の量をのぞいて $\omega_0 v_P(\alpha_0)$, $\zeta_0 v_P(\alpha_0)$ そして $(\omega_0+\zeta_0)v_P(\alpha_0)$ の次数で割ることがわかる．ゆえにこの場合も

P は J_0 の分子に高々有限の次数でしか現われない．

これで J_0 が standard であるという（iv）の主張は証明された．

このことから，もし $$A=\prod A_j^{\omega_j}$$

が A を素の divisor の巾の積として表わしたものであれば，

11.16 $$\sigma(A)=\prod(\sigma(A_j))^{\omega_j}$$

が成立することがわかる．

われわれは $\sigma(A)$ の定義を 11.16 により分数 divisor にも拡張することにする．σ はこうしてもやはり乗法的である．さらにどんな $K^\times$ の元 α をとってきても $\sigma([\alpha])=1$ である．ここに 1 は $R_{+\infty}$ の単位元である．このことは 11.8 と 11.9 から容易にわかる．なんとなれば，もし $[\alpha]=A/B$ で A, B が共通の divisor をもたないとすれば，

$$\sigma([\alpha])=\sigma(A)/\sigma(B)$$

$$\sigma(A)=H(\alpha)=H(1/\alpha)=\sigma(B)$$

であるから.

さて，われわれが整の divisor A の大きさを定義するとき，われわれは A の素の因子が $[\alpha]$, $[\beta]$ のなかにちょうど同じ次数で現われるようにした. しかしながら（i）と（ii）の証明をながめてみるとこの条件を改めることができることがわかる. かくして 11.2 **は 11.1 で定義される** $s(\alpha,\beta)$ **で** A **が** $[\alpha]$ **と** $[\beta]$ **の分子の最大公約 divisor であれば成立していることがわかる.** $|J_{\alpha,\beta}|$ の定義を考えたうえで，つぎのように書いてよい.

11.17 $$s(\alpha,\beta)=\prod\max(\min(|\alpha|_P,1),\min(|\beta|_P,1))$$

ここで P はアルキメディアン，アルキメディアンでないを問わず $^*k$ のすべての internal valuation を走るのである.

さて，α,β を $K^\times$ の 2 元として A と B をおのおの α,β の分母であるとする. E を A と B との最小公倍 divisor とせよ. したがって (A, B) を A と B との最大公約 divisor とすれば

$$E=AB/(A,B)$$

となり，それから（11.7 参照）

$$\sigma(A)=\theta(\prod\min(|\alpha^{-1}|_P,1))$$

$$\sigma(B)=\theta(\prod\min(|\beta^{-1}|_P,1))$$

$$\sigma((A,B))=s(\alpha^{-1},\beta^{-1})=\prod\max(\min(|\alpha^{-1}|_P,1),\min(|\beta^{-1}|_P,1))$$

となり，それゆえに

$$\begin{aligned}\sigma(E)=\frac{\sigma(A)\sigma(B)}{\sigma((A,B))}&=\theta((\prod\min(\min(|\alpha^{-1}|_P,1),\ \min(|\beta^{-1}|_P,1))^{-1})\\&=\theta((\prod\min(|\alpha^{-1}|_P,|\beta^{-1}|_P,1))^{-1})\\&=\theta(\prod\max(|\alpha|_P,|\beta|_P,1))\end{aligned}$$

しかしながら $\prod\max(|\alpha|_P,|\beta|_P,1)$ は定義により（S. Lang Diophantine Geometory 参照）$(\alpha,\beta,1)$ の高さ $H(\alpha,\beta,1)$ に等しい. したがって

11.18 $$\sigma(E)=\theta(H(\alpha,\beta,1))$$

われわれは §13 で 11.18 を用いることにする.

われわれは素の divisor A に対して $\sigma(A)$ を A をひき起こす valuation P_j の集合を用いて簡単に定義するわけにはいかない．なぜならばこの集合は external であって，この集合について $\prod(NP_j)^{-\nu_j}$ は存在するとはかぎらないからである．

12. divisor の大きさとその絶対値

q を 1 より大きな実数とし，A を関数体としての K の divisor で $A=\prod A_j^{\nu_j}$ が A の素の divisor の積として表わしたものとする．

このとき A の絶対値 $|A|$ をつぎのごとく定義する．

12.1 $$|A|=q^{-\Sigma\nu_j f_j}$$

ここで f_j は A の次数，すなわち k の上の A_j の剰余類体の次数であるとする．

どんな $K^{\times}$ の元 α をとっても $|[\alpha]|=1$ となる．すでに証明したように $\sigma([\alpha])=1$ であり，$\sigma([\alpha])$ 自身 α の絶対値の積の一種であるから，われわれは $|A|$ と $\sigma(A)$ との間に直接な関係があることを期待してよいわけである．しかし一方 $\sigma(A)$ は実数ではない（nonstandard な実数ですらない）したがってわれわれは

E. Artin and G. Whaples, Axiomatic characterization of fields by the product formula for valuations, Bulletin of the American Mathematical Society, vol. 51, 1945, pp. 469—492

の結果を応用することはできない．しかしわれわれは期待した関係が存在することを証明するのにこの論文のアイディアを用いることにする．

定理 6 K を k の上の有理関数体とする．したがって $K=k(\omega)$ で $\omega\in{}^*k-k$ とする．このとき正の無限大の $\lambda\in{}^*R$ が存在して，K のすべての divisor A について

12.2 $$\sigma(A)=\theta(|A|^{\lambda})$$

が成立する．

（証明） $\tau=\omega^{-1}$ は K における次数 1 の素の divisor すなわち無限大にお

ける divisor を作る．われわれはこれを A_∞ によって表わすことにする．そうすると

$$|A_\infty|=q^{-1}$$

となる．θ を以前と同じく $^*R_+ \to R_{+\infty}$ への準同型写像として，$a\in{}^*R_+$ なる a を選んで

$$\sigma(A_\infty)=\theta(a)$$

となるようにする．そして

$$\lambda=-\log_q a$$

とおく．

A_∞ はある K の valuation によってひき起こされるのであるから，a は負の無限大でなければならず，したがって λ は正の無限大である．さらに

$$a=q^{-\lambda}$$

したがって

$$\sigma(A_\infty)=\theta(q^{-\lambda})=\theta(|A_\infty|^\lambda)$$

したがって 12.2 は $A=A_\infty$ に対しては成立する．

われわれは，12.2 が K のほかのすべての divisor に対しても成立することを証明しよう．

σ, θ, $|\ \ |$ がすべて乗法的であるから素の A に対してのみ証明すれば十分である．したがって A を A_∞ 以外の K の素の divisor であるとしよう．したがって A は $k[x]$ の既約な多項式 $p(x)$ によってあたえられる（§10 参照）．このとき $n\geq 1$ を $p(x)$ の次数とすれば $|A|=q^{-n}$ となる．したがってわれわれの証明すべきことは

$$\sigma(A)=\theta(q^{-n\lambda})=(\theta(q^{-\lambda}))^n=(\sigma(A_\infty))^n=\sigma(A_\infty{}^n)$$

である．すなわちいいかえれば

$$\sigma(A/A_\infty{}^n)=1$$

である．しかしこれは $[p(\omega)]=A/A_\infty{}^n$ と $\sigma([p(\omega)])=1$ から明らかである．

さてわれわれは一般の場合 K が k の上の超越次数 1 の関数体であって $K\subset{}^*k$ である場合を考えよう．$K^\times$ の任意の元 α と K の任意の素の divisor Q に対して

$$\sigma_Q(\alpha)=(\sigma(Q))^\nu\in R_{+\infty}$$

と定義しよう．ここに ν は α の valuation Q の exponential な値であると

する．すなわち

$$\nu = W_Q(\alpha)$$

したがって σ_Q は乗法的である．すなわち

$$\sigma_Q(\alpha\beta) = \sigma_Q(\alpha)\sigma_Q(\beta)$$

また，素な Q（さらに一般に整な Q）については

$$\sigma(Q) \leq 1$$

となる．ゆえに $\alpha, \beta, \alpha+\beta \in K^{\times}$ ならば

$$W_Q(\alpha+\beta) \geq \min(W_Q(\alpha), W_Q(\beta))$$

から

$$\sigma_Q(\alpha+\beta) \leq \max(\sigma_Q(\alpha), \sigma_Q(\beta))$$

がでる．

任意の $\omega \in K-k$ に対して $K'=k(\omega)$ とおけば，定理6 を $k(\omega)$ に適用することができる．われわれはふたたび $\tau=\omega^{-1}$ によって定まる divisor を A_∞ で表わすことにする．われわれはさらに K のすべての divisor A に対して $\lambda(A) \in {}^*R$ を $\sigma(A) = \theta(|A|^{\lambda(A)})$ が成立するように選ぶことにする．$\lambda(A)$ は有限の ${}^*R$ の元を（加法の意味で）のぞいて一意的に定まることは明らかであろう．われわれはまだ K のすべての素の divisor が ${}^*k$ のある valuation からひき起こされることを証明してないから，いまのところ $\lambda(A)=0$ ということがありうるということを注意しておこう．

$\alpha_1, \cdots, \alpha_f$ を K の $k(\omega)$ の上の基底（basis）であるとしよう．われわれは α_j を適当に選んで，$\alpha_1, \cdots, \alpha_f$ が A_∞ を割らない（ここでは A_∞ は K の divisor）K のすべての divisor に対して整であるようにできる．すなわちそのように Q に対しては

$$\sigma_Q(\alpha_j) \leq 1 \qquad j=1, \cdots, f$$

となる．

いま正の自然数 d を固定したとき，

$$S_d = \{\sum_{j=1}^{f} p_j(\omega)\alpha_j \mid p_j(\omega) \in k[\omega] \text{ で } (p_j(\omega) \text{ の次数}) \leq d\}$$

と定義しよう．このとき S_d は k の上の階数（rank）$(d+1)f$ なるベクトル空間となる．

どんな $\xi\in S_d, \xi\neq 0$ とどんな K の素の divisor Q をとってきても

$$\sigma_Q(\xi)=\sigma_Q(\sum_{j=1}^{f} p_j(\omega)\alpha_j)\leq \max(\sigma_Q(p_j(\omega)),\sigma_Q(\alpha_j))$$

となる．しかし Q は A_∞ を割らないから

$$\sigma_Q(p_j(\omega))\leq 1$$

そしてさらに $$\sigma_Q(\alpha_j)\leq 1.$$

ゆえにつぎの式が得られた．

12.3 $$\sigma_Q(\xi)\leq 1$$

いまつぎのごとくおこう．

12.4 $$A_\infty=\prod Q_{i\infty}^{e_i}$$

ここに A_∞ は K の divisor と考えている．そして 12.4 は A_∞ の素の divisor への分解である．

いま Q を $Q_{i\infty}$ の 1 つとする．そのとき

$$\sigma_Q(\xi)\leq \max_j(\sigma_Q(p_j(\omega)),\sigma_Q(\alpha_j))$$

が成立しており，さらに $W_Q(p_j(\omega))\leq W_Q(\omega^d)$

ゆえに $$\sigma_Q(p_j(\omega))=\sigma_Q(\omega^d).$$

また $Q_{i\infty}$ は A_∞ を割るから

$$W_Q(\alpha_j)\geq W_Q(\omega^t),\ j=1,\cdots,f$$

が十分大きな自然数 t に対して成立する．このとき $\sigma(\alpha_j)\leq\sigma(\omega^t)$ であるから，つぎが得られる．

12.5 $$\sigma_Q(\xi)\leq\sigma_Q(\omega^{t+d})$$

ここで t は ω のとり方に依存するが d にはよらない．

さていま Q は K の任意の素の divisor として d_Q をその degree とする．このとき正の自然数 r が存在してつぎの条件をみたす．

$$rd_Q<(d+1)f\leq(r+1)d_Q$$

すべての $\xi\in S_d$ に対して $W_Q(\zeta)\leq W_Q(\xi)$

になるように S_d の元 ζ を選べる．なぜならば Q は discrete であり，どんな $\xi \in S_d$ に対しても

$$W_Q(\xi) \geq \min(\omega^m \alpha_j) \qquad m=0,1,\cdots,d \quad j=1,\cdots,f$$

となるからである．

この ζ に対しては，任意の $\xi \in S_d$ に対して

$$W_Q(\xi/\zeta) \geq 0$$

すなわち ξ/ζ はQ の v-環 v_Q に属することがわかる．

mod Q^r で考えると v_Q の rd_Q 以上の元が独立ではありえないから，$\xi_0 \in S_d$ なる元で

$$\xi_0/\zeta \equiv 0 \pmod{Q^r}$$

で $\xi_0 \neq 0$ なるものが存在する．したがって

$$W_Q(\xi_0/\zeta) \geq r$$

となる．

われわれは通例のように

$$|\alpha|_Q = q^{-W_Q(\alpha)d_Q}$$

と定義する．ゆえに

$$|\xi_0/\zeta|_Q \leq q^{-rd_Q} \leq \frac{q^{d_Q}}{q^{(r+1)d_Q}} \leq q^{d_Q-(d+1)f}$$

ゆえに
$$|\xi_0|_Q \leq q^{d_Q-(d+1)f}|\zeta|_Q$$

この不等式を $\lambda(Q)$ 乗して θ をほどこせば

12.6
$$\sigma_Q(\xi_0) \leq \theta(q^{(d_Q-(d+1)f)\lambda(Q)})\sigma_Q(\xi)$$

さてわれわれは 12.6 に $\xi=\zeta_0$ と K における $Q' \neq Q$ なるすべての divisor について，12.3 か 12.5 のいずれか適用できるほうをかけてつぎの式を得る．

12.7
$$\sigma_Q(\xi_0)\prod\sigma_{Q'}(\xi_0) \leq \theta(q^{(d_Q-(d+1)f)\lambda(Q)})\sigma_Q(\zeta)\prod\sigma_{Q'}(\omega^{t+d})$$

さて Q が A_∞ を割らないか，割るかによって

$$\sigma_Q(\zeta) \leq 1 \text{ かまたは } \sigma_Q(\zeta) \leq \sigma_Q(\omega^{t+d})$$

となる．いずれにしても 12.7 からつぎのものを得る．

12.8
$$\sigma_Q(\xi_0)\prod\sigma_{Q'}(\xi_0) \leq \theta(q^{(d_Q-(d+1)f)\lambda(Q)})\prod\sigma_{Q'}(\omega^{t+d})$$

この最後の $\prod$ について Q' は A_∞ のすべての素の divisor を走るものとす

る．同時に 12.8 の左側はちょうど $\sigma([\zeta_0])$ に等しく，これは前節の終りに示したように 1 となる．

さて任意の $Q'=Q_{t\infty}$ に対して $\mu(Q')$ を

12.9 $$\sigma_{Q'}(\omega)=\theta(q^{\mu(Q')})$$

によって定義しよう． $\mu(Q')$ は正の量をのぞいてしか一意的に定まらないがそれを適当に選ぶことにしよう．いずれにしても $\mu(Q')\geq 0$ としてよい．12.9 に代入してわれわれはつぎの式を得る．

12.10 $$1\leq\theta(q^{(d_Q-(d+1)f)\lambda(Q)+(t+d)\Sigma\mu(Q')})$$

この式から，この右辺の巾乗の形が負の無限大にはならないことがわかる．別のふうにいえば有限の $b\in{}^*R$ が存在してつぎの式が成立する．

12.11 $$(f-d_Q)\lambda(Q)-t\sum\mu(Q')+d(f\lambda(Q)-\sum\mu(Q'))<b$$

われわれはいまから $\sum\mu(Q')$ が正の無限大であることを証明しよう．このために P を $k(\omega)$ における valuation A_∞ をひき起こす $^*k$ の任意の valuation としよう．§10 からそのような valuation が存在することがわかる．このとき P は K における valuation Q' をひき起こし，この Q' は A_∞ の拡張になっている．いいかえれば Q' は K における divisor としての A_∞ を割る．どんな P も $\sigma(Q')$ にあたえる量は無限小であるから，$\sigma_{Q'}(\omega)$ が無限大であってしたがって $\mu(Q')$ が正の無限大であることがわかる．このことから $\sum\mu(Q')$ が正の無限大であることがでてくる．

12.11 にもどってわれわれはこの不等式が任意の正の自然数 d に対して d に依存する b に対して成立していることを注意しておく．

われわれはつぎにつぎの命題を証明しよう．

12.12 $f\lambda(Q)-\sum\mu(Q')\leq 0$ であるかまたは $f-\dfrac{1}{\lambda(Q)}\sum\mu(Q')$ は正の無限小で $\lambda(Q)$ は正の無限大である．

まず，$f\lambda(Q)-\sum\mu(Q')>0$ であると仮定しよう．このとき $\lambda(Q)$ は正の無限大である．さらに

$$f-\frac{1}{\lambda(Q)}\sum\mu(Q')>\varepsilon$$

で $\varepsilon\in R_+$ であるとしよう．このときは

$$\sum\mu(Q')<(f-\varepsilon)\lambda(Q)$$

これから 12.11 の右辺は

$$((f-d_Q)-t(f-\varepsilon)+d\varepsilon)\lambda(Q)$$

より大きいことがわかる．しかし d を十分大きくとることにより $\lambda(Q)$ の前の$(\cdots)$の値を1より大きくすることができる．このような d に対して 12.11 の左辺は $\lambda(Q)$ より大きくなり，したがって無限大となり矛盾が生じた．

さて $\alpha\in k(\omega)$，$\alpha\neq 0$ として B を $k(\omega)$ の素の divisor，$B=\prod B_j^{d_j}$ を B の K における素の divisor への分解とする．このときもし f_j が B_j の inertia の次数であれば，$k(\omega)$の valuation B においての α の絶対値を $|\alpha|_B$ とおくことにする．だから

$$|\alpha|_{B_j}=|\alpha|_B{}^{d_jf_j}$$

となる．これからつぎの式が得られる．

$$\sigma_{B_j}(\alpha)\equiv\theta(|\alpha|^{d_jf_j\lambda(B_j)})$$

12.1 とこれを比べて，$Q'=Q_j=B_j, A_\infty=B, \alpha=\omega$ ならば

$$\sigma_{Q_j}(\alpha)=\theta(q^{\mu(Q_j)})=\theta(|\alpha|_B{}^{\mu(Q_j)})$$

を得る．これから $d_jf_j\lambda(Q_j)-\mu(Q_j)$ が有限，したがって $\sum d_jf_j\lambda(Q_j)-\sum\mu(Q_j)$ が有限であることがわかる．$\sum\mu(Q_j)$ は前に $\sum\mu(Q')$ と書いたものである．$\sum\mu(Q_j)=\mu_\infty$ とおけば，μ_∞ は正の無限大である．

さて一般の $\alpha\in k(\omega), \alpha\neq 0$ について

$\sigma([\alpha])=1$ でありまたさらに

$$\sigma([\alpha])=\prod\sigma_{B_j}(\alpha)=\theta(\prod_B\prod_{B_j|B}|\alpha|_B{}^{d_jf_j\lambda(B_j)})$$

ここで最初の積では B_j は K のすべての divisor を走るものとする．したがって

12.13 $$\theta(\prod|\alpha|_B{}^{\sum_j d_jf_j\lambda(B_j)})=1$$

さて，とくに $\alpha=p(\omega)$ は素の divisor B をきめる既約多項式であるとする．このとき

$$[\alpha]=BA_\infty{}^{-n}$$

ここに n は $p(\omega)$ の次数である．したがって 12.4 の記号を用い Q_j の inertia の次数を g_j と書けば

$$|\alpha|_B=q^{-n},\quad |\alpha|_{A\infty}=q^n$$

したがって 12.13 から

$$Q(q^{-n(\Sigma d_j f_j \lambda(B_j)-\Sigma e_j g_j \lambda(Q_j))})=1$$

これからつぎのことが得られる．

12.14 $\sum d_j f_j \lambda(B_j)-\sum e_j g_j \lambda(Q_j)$ は有限である．

さらに上にのべたことからわかるように 12.14 の第 2 の $\sum$ の項と μ_∞ とは有限の量しか異ならないから，この項を μ_∞ でとりかえてもよい．したがって

12.15 $\sum d_j f_j \lambda(B_j)-\mu_\infty$ は有限である．

同時に 12.12 の前半か後半のいずれかが各々の $B_i=Q$ に適用でき，$\sum\mu(Q')=\mu_\infty$ であるから，まずすべての B_i について $f\lambda(B_i)-\mu_\infty\leqq 0$ として

12.16 $\sum d_j f_j \lambda(B_j)-f\lambda(B_i)$ は負の無限大ではない．

l を適当に選んで $\lambda(B_i)$ が $i=l$ で最大であるようにし，$\sum d_j f_j=f$ を用いて 12.16 から

12.17 $\sum_j d_j f_j \lambda(B_j)-f\lambda(B_l)=\sum_j d_j f_j(\lambda(B_j)-\lambda(B_l))$ は負の無限大ではない．

この右辺のどの項も正ではないからおのおのの項が有限であることがでてくる．ゆえに $\lambda(B_j)=\lambda(B_l)+b_j$ と書けば b_j は有限である．12.15 に代入してつぎのことがわかる．

$$f\lambda(B_l)-\mu_\infty \text{ は有限である．}$$

それゆえ $\lambda(B_l)$ は正の無限大で $f-\dfrac{\mu_\infty}{\lambda(B_l)}$ は無限小である．しかしある i に対して $f\lambda(B_i)-\mu_\infty>0$ ならば，同じ結論を得る．なぜならばこのときは $i=l$ に対しては成立しており，12.12 の後半が適用できるからである．いずれにしても $\lambda(B_l)$ で 12.15 を割って

$$\sum d_j f_j \frac{\lambda(B_j)}{\lambda(B_l)}-\frac{\mu_\infty}{\lambda(B_l)}\simeq 0$$

ゆえに

$$\sum d_j f_j \frac{\lambda(B_j)}{\lambda(B_l)}-f\simeq 0$$

そして

12.18 $$\sum d_j f_j\left(\frac{\lambda(B_j)}{\lambda(B_l)}-1\right)\simeq 0$$

しかし $\lambda(B_j)\leq\lambda(B_l)$ はすべての j に対して成立するから $\dfrac{\lambda(B_j)}{\lambda(B_l)}-1$ はいつでも無限小であり

$$\frac{\lambda(B_j)}{\lambda(B_l)}\simeq 1.$$

$\dfrac{\mu_\infty}{\lambda(B_l)}\simeq f$ で割って，つぎのものを得る．

12.19 $$\frac{\lambda(B_j)}{\mu_\infty}\simeq\frac{1}{f}$$

さてすべての K の素の divisor $Q=B_j$ は $k(\omega)$ の divisor B を割る．ここで B は valuation として B_j を $k(\omega)$ に制限して得られる．ゆえに，12.19 を K の 2 つの素の divisor Q, Q' に適用して，つぎの式が得られる．

12.20 $$\frac{\lambda(Q')}{\lambda(Q)}\simeq 1$$

したがってつぎの定理が得られた．

定理 7 Q, Q' を K の 2 つの素の divisor として，$\lambda(Q)$, $\lambda(Q')$ をつぎの $^*R$ の元とする．

$\sigma(Q)=\theta(|Q|^{\lambda(Q')})$ で $\sigma(Q')=\theta(|Q'|^{\lambda(Q')})$ このとき $\lambda(Q),\lambda(Q')$ は正の無限大であり，$\lambda(Q')/\lambda(Q)$ は 1 に無限に近い（差が無限小である）．

系 定理 7 はすべての K の整の divisor Q, Q' に対して成立する．

（証明） Q が素であって，Q' が任意の整の divisor のときに証明すれば十分である．

$Q'=\prod Q_j^{\nu_j}$ とし d' を Q' の次数，d_j を Q_j の次数とする．λ_j を適当に選べば

$$\sigma(Q_j)=\theta(|Q_j|^{\lambda_j})$$

ゆえに

$$\lambda_j=\lambda(Q)(1+\varepsilon_j)$$

とおけば ε_j は無限小である．ゆえに

$$\sigma(Q')=\prod(\sigma(Q_j))^{\nu_j}=\theta(\prod|Q_j|^{\lambda_j\nu_j})$$
$$=\theta(|Q'|^{\lambda(Q)})\theta(\prod|Q_j|^{\lambda(Q)\nu_j\varepsilon_j})$$

また仮定により

$$\sigma(Q')=\theta(|Q'|^{\lambda(Q')})$$

でありゆえに　$\theta(|Q'|^{\lambda(Q)-\lambda(Q')}\prod|Q_j|^{\lambda(Q)\nu_j\varepsilon_j})=1$

$|Q'|=q^{-d'}, |Q_j|=q^{-d_j}$ であることを思いだせば

12.21　$d'(\lambda(Q)-\lambda(Q'))+\sum_j \lambda(Q)d_j\nu_j\varepsilon_j$ は有限

$\lambda(Q)$ で割れば　$d'\left(1-\dfrac{\lambda(Q')}{\lambda(Q)}\right)+\sum_j d_j\nu_j\varepsilon_j\simeq 0$

しかし $\varepsilon_j\simeq 0$ であるから　$1-\dfrac{\lambda(Q')}{\lambda(Q)}\simeq 0$

となって証明された.

系　K のすべての素の divisor Q は $^*k$ のある valuation P によってひき起こされる.

このことは $\lambda(Q)$ が無限であるから $\sigma(Q)$ を定義する積が空なものの積ではありえないことからわかる.

12.1 の用いた記号を §11, §12 の定義からながめて $q=e$ とおけば定理 7 の系からつぎの形の定理を得る.

定理 8　AをKにおける 2 つの divisor $[\alpha]$, $[\beta]$ の分子の最大公約 divisor とする. $A\neq 1$ としてdをAの次数とする. A' をKにおける divisor $[\alpha']$, $[\beta']$ の分子の最大公約 divisor でやはり $A'\neq 1$ で A' の次数を d' とする. そのとき

12.22　$$\frac{\log s(\alpha',\beta')}{\log s(\alpha,\beta)}\simeq\frac{d'}{d}$$

13. standard な理論への移行

この節においてわれわれはわれわれの理論から代数曲線の有理点に関しての基本的な不等式がただちに導かれることを示すことにする.

最初に実数体 R についてどうなっているか考えてみよう. 最初に $\{s_n\}$, $\{s_n'\}$ は 2 つの正の実数列で $n\to\infty$ のとき $\{s_n\}$ と $\{s_n'\}$ はともに 0 に近づくか, ともに ∞ に近づくものとする. このときわれわれは

$$\{s_n\}\approx\{s_n'\}$$

と書くことにする.

さていま $\{s_n\}$ と $\{s_n'\}$ についてのつぎの命題を考える.

13.1　どんな $\varepsilon>0$ をとっても, 正の定数 c_1, c_2 があって

$$c_1 s_n^{1-\varepsilon} \leq s_n' \leq c_2 s_n^{1+\varepsilon}$$

この 13.1 はつぎの命題と同等である.

13.2
$$\frac{\log c_1}{\log s_n'} + (1-\varepsilon)\frac{\log s_n}{\log s_n'} \leq 1 \leq \frac{\log c_2}{\log s_n'} + (1+\varepsilon)\frac{\log s_n}{\log s_n'}$$

$\{s_n\}$ と $\{s_n'\}$ は同時に 0 か ∞ に近づくからこれはさらにつぎの命題と同等である.

13.3
$$\lim_{n\to\infty}\frac{\log s_n}{\log s_n'} = 1$$

なぜならば, もし 13.3 がみたされていれば, 十分大きな n に対して $\log s_n/\log s_n'$ は 1 に近い. したがって 13.2 はたしかにみたされる. われわれは c_1, c_2 を上手にとって 13.2 を残りの有限個の n についても成立するようにすればよい. 逆も同じように簡単に証明される.

こんどは $\{s_n\}, \{s_n'\}$ はいままで通りとして, $^*R$ に移行しよう. われわれは無限の ω に対して s_ω と s_ω' とが同時に無限小であることがわかる. ここで 13.3 はつぎの 13.4 でおきかえられる.

13.4
$$\frac{\log s_\omega}{\log s_\omega'} \simeq 1$$

さて k は代数体で $f(x, y) \in k[x, y]$ で Γ は $f(x, y)=0$ によってあたえられる既約の代数曲線であるとしよう. さらに Γ は $k\times k$ の相異なる無限の点 $(\xi_n, \eta_n), n=0, 1, 2, \cdots$ をもっているものとする. 前に証明したように (§6 参照), $(\xi_\omega, \eta_\omega)$ は Γ の ω が無限大ならば generic point である. したがって $K=k(\xi_\omega, \eta_\omega) \subset {}^*k$ は前節で考えた関数体になっている.

さて $g(x, y) \in k(x, y)$ で $g(\xi_\omega, \eta_\omega)$ は有限 (すなわち $g(x, y)$ の分母は f で割れない) で定数ではないものとする (すなわち k の元ではない). d_g を $g(\xi_\omega, \eta_\omega)$ の K における次数とする. このとき関数 divisor $[g]$ の分子もまた次数 d_g をもつ. §11 (11.7—11.9 参照) に示したように, $g(\xi_\omega, \eta_\omega)$ の高さは

13.5
$$H(g(\xi_\omega, \eta_\omega)) = (s(g(\xi_\omega, \eta_\omega), g(\xi_\omega, \eta_\omega)))^{-1}$$

によってあたえられる.

$h(x,y)\in k(x,y)$ を同じ条件をみたす関数でその次数が d_h とすれば

13.6 $$H(h(\xi_\omega,\eta_\omega))=(s(h(\xi_\omega,\eta_\omega),h(\xi_\omega,\eta_\omega)))^{-1}$$

$d_g>0, d_h>0$ であるから 13.5, 13.6 の左辺は無限小の逆数になっておりしたがって無限大である. 12.22 の右辺に $\alpha=\beta=g(\xi_\omega,\eta_\omega)$, $\alpha'=\beta'=h(\xi_\omega,\eta_\omega)$, $d=d_g$, $d'=d_h$ として代入すれば

13.7 $$\frac{\log(H(h(\xi_\omega,\eta_\omega)))^{1/d_h}}{\log(H(g(\xi_\omega,\eta_\omega)))^{1/d_g}}\simeq 1$$

が得られる. したがって本節の最初の議論を

$$s_n\simeq(H(g(\xi_\omega,\eta_\omega)))^{1/d_g} \text{ と } s_n'=(H(h(\xi_\omega,\eta_\omega)))^{1/d_h}$$

適用すれば (有限個の g または h が零になるところおよび無限大になる項はとりのぞいて考える) つぎの定理を得る.

定理 9 k は代数体で Γ は $f(x,y)=0, f(x,y)\in k[x,y]$ によってあたえられた既約な代数曲線であるとする. $g(x,y)$, $h(x,y)$ は $k(x,y)$ の元で Γ の関数体 K/k における像が有限で定数ではないものとし, その次数をおのおの d_g, d_h とする. (ξ_n, η_n) は Γ の $k\times k$ の点であってさらに $g(\xi_n,\eta_n)$, $h(\xi_n,\eta_n)$ はすべて無限でもなく零でもないものとする. このとき

$$(H(g(\xi_n,\eta_n)))^{1/d_g}\approx(H(h(\xi_n,\eta_n)))^{1/d_h}$$

この定理が standard な定理, すなわち普通の数学の定理であることを注意しておく. ここで用いられた "無限" および "有限" は普通の意味, すなわち $f(x,y)$ または $h(x,y)$ の分母に代入したあとで 0 になるようなベクトルがあることまたはないことを意味しているだけである.

さてこんどは E は関数 divisor $[\xi_\omega],[\eta_\omega]$ の分母の最小公倍 divisor とする. $\xi_\omega+r\eta_\omega$ を適当な $r\in k$ について考えれば, E の次数 d は Γ の order すなわち K の $k(\xi_\omega)$ の上の次数と等しいことがわかる. ゆえに 11.18 と 12.21 により

13.8 $$\frac{\log H(g(\xi_\omega,\eta_\omega))}{\log(H(\xi_\omega,\eta_\omega,1))^{d_g/d}}\simeq 1$$

が得られる.

かくしてつぎの定理が得られた．

定理 10　定理 9 の仮定のもとで，d を Γ の order とせよ．このとき

13.9 $$H(g(\xi_n, \eta_n)) \approx (H(\xi_n, \eta_n, 1))^{d_g/d}$$

さてこんどは $\xi_n = x_n/z_n$，$\eta_n = y_n/z_n$ で x_n, y_n, z_n は k の代数的整数とし，(x_n, y_n, z_n) は共通の約数をもたないものとする．このとき

13.10 $$H(\xi_n, \eta_n, 1) = H(x_n, y_n, z_n) \geq \prod{}' 1/3(|x_n|_P + |y_n|_P + |z_n|_P)$$

ここで $\prod'$ は積がアルキメディアン valuation だけについてとられることを意味する．さて $F(\xi_n, \eta_n)$ がすべての n に対して整であるとして $g(x, y) = 1/F(x, y)$ とせよ．さらに $\delta > 0$ なる実数があって，すべての n とすべての k のアルキメディアン valuation P について

$$|F(\xi_n, \eta_n)|_P > \delta$$

であるとせよ．このとき

13.11 $$\begin{aligned} H(g(\xi_n, \eta_n)) &= \prod \max(|g(\xi_n, \eta_n)|_P, 1) \\ &= \prod{}''\left(\left|\frac{1}{F(\xi_n, \eta_n)}\right|_P\right) \\ &= \left(\prod{}'\left(\left|\frac{1}{F(\xi_n, \eta_n)}\right|_P\right)\right)^{-1} \end{aligned}$$

ここに $\prod''$ は積がアルキメディアンでない valuation だけにとられることを意味し，$\prod'$ は以前と同じくアルキメディアン valuation だけについて考えることを意味している．

さてここで 13.9 を考えれば，あたえられた $\varepsilon > 0$ に対して $c > 0$ が存在してすべての n に対して

$$\left(\prod{}'\left(\left|\frac{1}{F(\xi_n, \eta_n)}\right|_P\right)\right)^{-1} \geq c\left(\prod{}'(|x_n|_P + |y_n|_P + |z_n|_P)\right)^{d_g/d - \varepsilon}$$

であることがわかる．したがってつぎの式が得られる．

13.12 $$\prod{}'\left|\frac{1}{F\left(\dfrac{x_n}{z_n}, \dfrac{y_n}{z_n}\right)}\right|_P \leq \frac{1}{c}\left(\prod{}'(|x_n|_P + |y_n|_P + |z_n|_P)\right)^{-d_g/d + \varepsilon}$$

ここで，もしのぞめば $\leq$ を $<$ でかえてもよい．この式は

C. L. Siegel: Über einige Anwendungen diophantischer Approximationen,

Abhandlungen der Preussischen Akademic der Wissenschaften, Physikal-isch-Mathematische Klasse, Berlin 1929, pp. 209—266 の基本的な不等式である.

ここでのべたことは A. Robinson の仕事である.

あとがき

この機会に‘ゲーデルの新しい公理について’のその後の発展で私が知っていることを報告しておきたい．ただし，全体の事情がどうなっているのか，ここに書くことが本文に書いたこととどのようなつながりがあるかなどということについては一切省略させていただいて関係のある1つの定理だけについてのべることにする．この問題が一段落したときにもう少しくわしい報告をするつもりでいるがそれまではこういう程度の報告で我慢していただきたい．

ここに書くことの記号その他はすべて小著『現代集合論入門』（日本評論社）によることにする．

いま f と g とが ${\omega_\alpha}^{\omega_\beta}$ の元であるとき，$f \leq g$ を（本文の記号法とは異なるが）

$$\forall \gamma < \omega_\beta (f(\gamma) \leqslant g(\gamma))$$

によって定義することにする．いまさらに ${\omega_\alpha}^{\omega_\beta}$ の部分集合 M があたえられたときに，

$$M \text{ が } {\omega_\alpha}^{\omega_\beta} \text{ の major な部分集合である}$$

ということを

$$\forall f \in {\omega_\alpha}^{\omega_\beta} \exists g \in M (f \leq g)$$

によって定義することにする．

ここでわれわれがおもに問題にする命題はつぎの ω_α，ω_β についての命題である．この命題を

$$A(\omega_\alpha,\ \omega_\beta)$$

と書くことにする．

“$\omega_\alpha{}^{\omega_\beta}$ の major な部分集合 M で

$$\overline{\overline{\{f\upharpoonright\gamma \mid f\in M\wedge\gamma<\omega_\beta\}}}\leq\aleph_\beta$$

であるようなものが存在する”

われわれの定理をのべるために，まず

$$2^{\underset{\smile}{\aleph_\alpha}}$$

を，すべての $\gamma<\alpha$ について，$2^{\aleph_\gamma}$ より小さくない最小の濃度数として定義する．さらに $$2^{\underset{\smile}{\aleph_0}}$$
は $\aleph_0$ と定義することにする．われわれの目的はつぎの定理である．

定理 $$2^{\underset{\smile}{\aleph_\alpha}}<cf(\aleph_\beta)$$

の仮定のもとで

$$A(\omega_\alpha,\ \omega_\beta)\ \rightarrow\ 2^{\underset{\smile}{\aleph_\alpha}}\leqslant\aleph_\beta$$

（証明） いま $\gamma<\omega_\alpha$ なる任意の γ と，$g:\gamma\rightarrow 2$ なる任意の関数 g について U_g を

$$U_g=\{f\in 2^{\omega_\alpha}\mid f\upharpoonright\gamma=g\}$$

によって定義し，2^{ω_α} の位相を基本近傍系を

$$\{U_g\mid\exists\gamma<\omega_\alpha(g:\gamma\rightarrow 2)\}$$

とあたえることによって定義する．

$$2^{\underset{\smile}{\aleph_\alpha}}<cf(\aleph_\beta)$$

の仮定のもとで，この位相空間 2^{ω_α} はつぎのような初等的な性質をみたす．この初等的な性質はここでは仮定して，定理の証明がすんだあとでその証明をすることにする．

1. $F_\gamma(\gamma<\omega_\beta)$ をこの空間の閉集合で

$$F_0\supseteq F_1\supseteq\cdots\supseteq F_\gamma\supseteq\cdots\qquad(\gamma<\omega_\beta)$$

がみたされているものとする．このとき，

$$\gamma_0<\omega_\beta$$

で $$F_{\gamma_0}=F_{\gamma_0+1}=\cdots=F_\gamma=\cdots\qquad(\gamma_0\leqslant\gamma<\omega_\beta)$$

をみたすものが存在する．

2.　Fがこの空間の閉集合で　$\overline{\overline{F}} > 2^{\aleph_\alpha}$

であれば，閉集合 $s(\gamma)$ $(\gamma < \omega_\alpha)$ であって

2.1　$$\gamma_1 < \gamma_2 < \omega_\alpha \to s(\gamma_1) \subseteq s(\gamma_2)$$

2.2　$$\bigcup_{\gamma < \omega_\alpha} s(\gamma) = 2^{\omega_\alpha}$$

2.3　$$\overline{\overline{F - s(\gamma)}} > 2^{\aleph_\alpha} \quad (\gamma < \omega_\alpha \text{ について})$$

さていま M を $A(\omega_\alpha, \omega_\beta)$ のなかで M と書かれた集合であるとして，

N を　$$N = \{f \upharpoonright \gamma \mid f \in M \wedge \gamma < \omega_\beta\}$$

によって定義し，さらに　$\gamma < \omega_\beta$

なる γ について N_γ を

$$N_\gamma = \{g \in N \mid \mathrm{dom}(g) = \gamma\}$$

によって定義する．　$\overline{\overline{N_\gamma}} < \aleph_\beta$

となるから，N_γ の元を重複を許して ω_β なる順序型に整列してそれを

$$g_{\gamma 0},\ g_{\gamma 1}, \cdots,\ g_{\gamma \delta}, \cdots \quad (\delta < \omega_\beta)$$

とすることにする．

いまわれわれは　$s(\gamma, \delta)$

なる 2^{ω_α} の部分集合をすべての $\gamma < \omega_\beta$ とすべての $\delta < \omega_\alpha$ について定義していくのであるが，この $s(\gamma, \delta)$ は少なくともつぎの性質をみたすものとする．

3.1　$s(\gamma, \delta)$ は 2^{ω_α} の閉集合である．

3.2　$$\delta_1 < \delta_2 < \omega_\alpha \to s(\gamma, \delta_1) \subseteq s(\gamma, \delta_2)$$

3.3　$$\bigcup_{\delta < \omega_\alpha} s(\gamma, \delta) = 2^{\omega_\alpha}$$

ここで $\omega_\beta \times \omega_\beta$ を ω_β に1対1 onto に写像する関数

$$j$$

とその逆関数　$k_1,\ k_2$

とを用いるが，われわれが以下に用いる性質はつぎのものである．

4.1 $$j : \omega_\beta \times \omega_\beta \xrightarrow[\text{onto}]{1:1} \omega_\beta$$

4.2 $$\gamma_1,\ \gamma_2 < \omega_\beta \to k_1(j(\gamma_1,\ \gamma_2)) = \gamma_1 \\ \wedge k_2(j(\gamma_1,\ \gamma_2)) = \gamma_2$$

4.3 $$\gamma < \omega_\beta \to j(k_1(\gamma),\ k_2(\gamma)) = \gamma$$

4.4 $$\gamma < \omega_\beta \to k_1(\gamma) \leqslant \gamma$$

われわれは $s(\gamma,\ \delta)$ を γ についての超限帰納法で定義してゆくことにする．そのためすべての $\eta < \gamma$ なる η と $\delta < \omega_\alpha$ なる δ については $s(\eta,\ \delta)$ が定義できているものとして，$s(\gamma,\ \delta)$ をすべての

$$\delta < \omega_\alpha$$

について定義することにする．まず

$$\sigma(\gamma) = \bigcap_{\eta < k_1(\gamma)} s(\eta,\ g_{k_1(\gamma)k_2(\gamma)}(\eta))$$

によって定義する．ここで場合を 2 つに分けて定義をすることにする．

その 1）　$\overline{\overline{\sigma(\gamma)}} \leqslant 2^{\aleph_\alpha}$　のとき

このときはすべての $\delta < \omega_\alpha$ について

$$s(\gamma,\ \delta) = 2^{\omega_\alpha}$$

と定義する．

その 2）　$\overline{\overline{\sigma(\gamma)}} > 2^{\aleph_\alpha}$　のとき

このときは 2.1，2.2，2.3 をみたす $s(\gamma,\ \delta)$ をつくる．すなわちつぎの条件をみたすようにする．

5.1 $$\delta_1 < \delta_2 < \omega_\alpha \to s(\gamma,\ \delta_1) \subseteq s(\gamma,\ \delta_2)$$

5.2 $$\bigcup_{\delta < \omega_\alpha} s(\gamma,\ \delta) = 2^{\omega_\alpha}$$

5.3 $$\overline{\overline{\sigma(\gamma) - s(\gamma,\ \delta)}} > 2^{\aleph_\alpha} \qquad (\delta < \omega_\alpha)$$

さて準備がすべて整ったので証明をすることにしよう．

$$2^{\omega_\alpha} = \bigcap_{\gamma < \omega_\beta} \bigcup_{\delta\ \omega_\alpha} s(\gamma,\ \delta) \qquad (5.2 \text{ により})$$

$$= \bigcup_{f \in \omega_\alpha{}^{\omega_\beta}} \bigcap_{\gamma < \omega_\beta} s(\gamma,\ f(\gamma)) \qquad (\text{選択公理})$$

$$(f \leq g \rightarrow \forall\gamma < \omega_\beta(s(\gamma, f(\gamma)) \subseteq s(\gamma, g(\gamma)))\text{ より})$$

$$= \bigcup_{f\in M} \bigcap_{\gamma<\omega_\beta} s(\gamma, f(\gamma))$$

ところで 1. により $\gamma_f < \omega_\beta$ なる γ_f で

$$\bigcap_{\gamma<\omega_\beta} s(\gamma, f(\gamma)) = \bigcap_{\gamma<\gamma_f} s(\gamma, f(\gamma))$$

をみたすものがある．この γ_f をとれば結局

$$2^{\omega_\alpha} = \bigcup_{f\in M} \bigcap_{\gamma<\gamma_f} s(\gamma, f(\gamma))$$

$$= \bigcup_{g\in N'} \bigcap_{\mathrm{dom}(g)} s(\gamma, g(\gamma))$$

ここで N' はつぎのごとく定義される．

$$N' = \{g \in N \mid \exists f \in M(\mathrm{dom}(g) = \gamma_f \wedge g = f \upharpoonright \gamma_f)\}$$

ところで $\overline{\overline{N'}} \leqslant \aleph_\beta$ は明らかであるからつぎのことを証明すれば定理の証明は終る．

$$\overline{\overline{\bigcap_{\gamma<\gamma_f} s(\gamma, f(\gamma))}} \leqslant 2^{\aleph_\alpha}$$

さてこのことを帰謬法によって証明することにして，これが成立していないと仮定してまず，　$\gamma_1 = \gamma_f$,　$g_{\gamma_1\gamma_2} = f \upharpoonright \gamma_f$

によって，γ_1, γ_2 を定義すると

$$\phi = \bigcap_{\gamma<\gamma_f} s(\gamma, f(\gamma)) - \bigcap_{\gamma<\omega_\beta} s(\gamma_1, f(\gamma)) \qquad (\gamma_f\text{ の定義})$$

$$= \bigcap_{\gamma<\gamma_1} s(\gamma, g_{\gamma_1\gamma_2}(\gamma)) - \bigcap_{\gamma<\omega_\beta} s(\gamma, f(\gamma)) \qquad (\gamma_1, \gamma_2\text{ の定義})$$

$$\supseteq \sigma(j(\gamma_1, \gamma_2)) - s(j(\gamma_1, \gamma_2), f(j(\gamma_1, \gamma_2)))$$

(σ の定義と，$\bigcap$ をその 1 つの成員でおきかえたこと)

ところで最後の式の濃度は $2^{\aleph_\alpha}$ より大きく，これが空集合であるからこれは矛盾であって定理は証明された．

系 1　　$\aleph_0 < cf(\aleph_\beta)$

であれば

$$A(\omega,\ \omega_\beta)\ \to\ 2^{\aleph_0} \leqslant \aleph_\beta$$

系 2
$$2^{\aleph_\alpha} < cf(\aleph_\beta)$$

であれば
$$A(\omega_{\alpha+1},\ \omega_\beta)\ \to\ 2^{\aleph_{\alpha+1}} \leqslant \aleph_\beta$$

さてつぎに先に仮定した 2^{ω_α} の初等的な性質を $2^{\aleph_\alpha}_{\smile} < cf(\omega_\beta)$ の仮定のもとで証明することにする．

定理 1　位相空間 2^{ω_α} の基本近傍系の濃度は $2^{\aleph_\alpha}_{\smile}$ である．

(証明)
$$\overline{\overline{\bigcup_{\gamma<\omega_\alpha} 2^\gamma}} \leqslant 2^{\aleph_\alpha}_{\smile}\cdot\aleph_\alpha = 2^{\aleph_\alpha}_{\smile}$$

定理 2　この空間のすべての基本近傍は閉集合でもある（近傍だから開集合であることは勿論である）．

(証明)　明らかであるから略す．

定理 3　$F_\gamma\ (\gamma<\omega_\beta)$ を 2^{ω_α} の閉集合で
$$F_0 \supseteq F_1 \supseteq \cdots \supseteq F_\gamma \supseteq \cdots \qquad (\gamma<\omega_\beta)$$
が成立しているとすると，$\gamma_0<\omega_\beta$ で
$$F_{\gamma_0} = F_{\gamma_0+1} = \cdots = F_\gamma = \cdots \qquad (\gamma_0 \leqslant \gamma < \omega_\beta)$$
をみたす γ_0 が存在する．

(証明)　すべての基本近傍を $2^{\aleph_\alpha}_{\smile}$ の順序型に整列して
$$G_0,\ \cdots,\ G_\delta,\ \cdots \qquad (\delta < 2^{\aleph_\alpha}_{\smile})$$
とする．すべての $\delta<2^{\aleph_\alpha}_{\smile}$ について
$$f(\delta) = \mu\gamma(G_\beta \frown F_\gamma = \phi)$$
と定義して
$$\gamma_0 = \sup_{\delta<2^{\aleph_\alpha}_{\smile}} f(\delta)$$
と定義すれば，γ_0 が定理をみたすことは明らかであろう．

定義　2^{ω_α} の部分集合 F について F^* を
$$F^* = \{f \in 2^{\omega_\alpha} \mid f \text{ のすべての近傍 } U \text{ について } \overline{\overline{U \frown F}} > 2^{\aleph_\alpha}_{\smile} \text{ が成立する}\}$$

によって定義する．さらに閉集合 F が perfect であるということを

$$F = F^*$$

であることと定義する．

定理 4　F を閉集合で，G を

$$G = \bigcup \{U| \text{（}U\text{は開集合）} > \overline{\overline{U \cap F}} \leqq 2^{\aleph_\alpha}\}$$

で定義すればつぎの性質が成立する．

1. $\overline{\overline{G \cap F}} \leqq 2^{\aleph_\alpha}$
2. $F^* = F - G$
3. F^* は perfect である．

（証明）　明らかに

$$G = \bigcup\{U| \text{（}U\text{ は基本近傍）} \wedge \overline{\overline{U \cap F}} \leqq 2^{\aleph_\alpha}\}$$

ゆえに

$$\overline{\overline{G \cap F}} = \overline{\overline{\bigcup_{\substack{U\text{は基本近傍} \\ \overline{\overline{U \cap F}} \leqq 2^{\aleph_\alpha}}} U \cap F}} \leqq 2^{\aleph_\alpha} \cdot 2^{\aleph_\alpha} = 2^{\aleph_\alpha}$$

2. と 3. とは 1. から明らかである．

定理 5　いま $f \in F^*$ とすれば，すべての $\gamma < \omega_\alpha$ についてつぎの条件をみたす δ が存在する．

1. $\gamma < \delta < \omega_\alpha$
2. $\overline{\overline{F \cap U_{(f \lceil \delta)^\frown 0}}} > 2^{\aleph_\alpha}$
3. $\overline{\overline{F \cap U_{(f \lceil \delta)^\frown 1}}} > 2^{\aleph_\alpha}$

ここに $(f \lceil \delta)^\frown n$ なる関数は $f \lceil \delta$ を δ における値が n という条件によって $\delta+1$ の上の関数に拡大してできた関数のことを意味する．

（証明）

$$F^* \cap U_{f \lceil (\gamma+1)} > 2^{\aleph_\alpha}$$

であるから，$U_{f \lceil (\gamma+1)} \cap F^*$ の元で f と異なるものが存在する．これを g としよう．

$$\delta = \mu\eta(f(\eta) \neq g(\eta))$$

とすればよい．

定理 6　$f \in F^*$ とすれば，基本近傍 $G_\gamma (\gamma < \omega_\alpha)$ でつぎの性質をみたすも

のが存在する．

1. $$\gamma_1 < \gamma_2 < \omega_\alpha \rightarrow G_{\gamma_1} \supseteq G_{\gamma_2}$$

2. $$\overline{\overline{F \cap G_\gamma}} > 2^{\aleph_\alpha}$$

3. $$\bigcap_{\gamma < \omega_\alpha} G_\gamma = \{f\}$$

（証明）　定理5を用いて，

$$\gamma_0,\ \gamma_1,\ \cdots,\ \gamma_\delta,\ \cdots < \omega_\alpha \qquad (\delta < \omega_\alpha)$$

でつぎの性質をみたすものを定義する．

1. $$\delta_1 < \delta_2 \rightarrow \gamma_{\delta_1} < \gamma_{\delta_2}$$

2. $$\overline{\overline{F \cap U_{(f \upharpoonright \gamma_\delta)^\frown 0}}} > 2^{\aleph_\alpha}$$

3. $$\overline{\overline{F \cap U_{(f \upharpoonright \gamma_\delta)^\frown 1}}} > 2^{\aleph_\alpha}$$

$$G_\delta = U_{f \upharpoonright (\gamma_\delta + 1)}$$

と定義すればよい．

定理 7　F を空でなく perfect とすれば閉集合 $s(\gamma)\ (\gamma < \omega_\alpha)$ でつぎの条件をみたすものが存在する．

1. $$\gamma_1 < \gamma_2 < \omega_\alpha \rightarrow s(\gamma_1) \subseteq s(\gamma_2)$$

2. $$\bigcup_{\gamma < \omega_\alpha} s(\gamma) = 2^{\omega_\alpha}$$

3. $$\overline{\overline{F - s(\gamma)}} > 2^{\aleph_\alpha} \qquad (\gamma < \omega_\alpha)$$

（証明）　$f \in F$ として，G_γ を定理6によって作り

$$s(\gamma) = \{f\} \cup (2^{\omega_\alpha} - G_\gamma)$$

とすればよい．

定理 8　F を閉集合で $\overline{\overline{F}} > 2^{\aleph_\alpha}$ とすれば，つぎの条件をみたす $s(\gamma)$ $(\gamma < \omega_\alpha)$ が存在する．

1. $$\gamma_1 < \gamma_2 < \omega_\alpha \rightarrow s(\gamma_1) \subseteq s(\gamma_2)$$

2. $$\bigcup_{\gamma < \omega_\alpha} s(\gamma) = 2^{\omega_\alpha}$$

3. $$\overline{\overline{F - s(\gamma)}} > 2^{\aleph_\alpha} \qquad (\gamma < 2^{\omega_\alpha})$$

（証明）　定理7より明らか．

索　引

著者：竹内外史

1926年　石川県に生まれる.
1947年　東京大学理学部数学科卒業.
1962年　東京教育大学教授.
現在　イリノイ大学教授.
主著　『数学基礎論』(共立)『現代集合論入門』(日本評論)

竹内外史著『数学基礎論の世界――ロジックの雑記帳から』

昭和47年5月30日　第1版第1刷

定価　1500円

検印省略

著者　竹内外史
発行者　小林昭一
発行所　日本評論社
160 東京都新宿区須賀町14
印刷　壮光舎
製本　青木製本株式会社